

**STATE LAW: SECURITY BREACH NOTIFICATION**

State	“Personal Information”	“Breach”	Exceptions	Destruction of Records and Security Policies	Disclosure of Breaches
<p><b>AZ</b></p> <p>ARIZ. REV. ST § 44-7501</p>	<p>Defined as an individual's first name or first initial and last name in combination with any one or more of the following data elements (i) SS number (ii) DL or state ID number (iii) the account or credit or debit card number in combination with any required security code, access code or password that would permit access to the individual's financial account.</p>	<p>Defined as “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 person 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.”</p>	<p>Good faith acquisition of personal information by an employee or agent of the person for the purposes of the person is not a breach of the security system if the personal information is not used for a purpose unrelated to the person or subject to further willful unauthorized disclosure.</p>		<p>If a Person becomes aware of an incident of unauthorized acquisition and access to unencrypted or unredacted computerized data that includes an individual's personal information, the person shall conduct a reasonable investigation to promptly determine if there has been a breach of the security system. If the investigation results in a determination that there has been a breach in the security system, the person shall notify the individuals affected.</p> <p>The notice shall be made in the most expedient manner possible and without unreasonable delay subject to the needs of law enforcement.</p> <p>Notification can be provided by: 1). Written notice; 2). Electronic notice; 3). Telephonic; or 4). Substitute notice. Substitute notice can be provided by 1). Email; 2). Conspicuous posting on a website; 3). Notification of statewide media.</p>

**STATE LAW: SECURITY BREACH NOTIFICATION**

State	“Personal Information”	“Breach”	Exceptions	Destruction of Records and Security Policies	Disclosure of Breaches
<p><b>AR</b> AR ST § 4-110-101 et seq.</p>	<p>“Personal information” means an individual's first name or first initial and his or her last name in combination with any one (1) or more of the following data elements when either the name or the data element is not encrypted or redacted: (A) SS number; (B) Driver's license number or Arkansas identification card number; (C) Account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; and (D) Medical information.</p>	<p>“Breach of the security of the system” means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person or business.</p>	<p>“Breach of the security of the system” does not include the good faith acquisition of personal information by an employee or agent of the person or business for the legitimate purposes of the person or business if the personal information is not otherwise used or subject to further unauthorized disclosure.</p>	<p>A person or business shall take all reasonable steps to destroy or arrange for the destruction of a customer's records within its custody or control containing personal information that is no longer to be retained by the person or business by shredding, erasing, or otherwise modifying the personal information in the records to make it unreadable or undecipherable through any means.</p> <p>A person or business that acquires, owns, or licenses personal information about an Arkansas resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.</p>	<p>Any person or business that acquires, owns, or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach of the security of the system to any resident of Arkansas whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time and manner possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system.</p> <p>For purposes of this section, notice should be provided by one (1) of the following methods: (1) Written notice; (2) Electronic mail notice if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001, as it existed on January 1, 2005; or (3) Substitute notice if the person or business demonstrates that:</p> <ul style="list-style-type: none"> <li>(i) The cost of providing notice would exceed two hundred fifty thousand dollars (\$250,000);</li> <li>(ii) The affected class of persons to be notified exceeds five hundred thousand (500,000); or</li> <li>(iii) The person or business does not have sufficient contact information.</li> </ul>

**STATE LAW: SECURITY BREACH NOTIFICATION**

State	“Personal Information”	“Breach”	Exceptions	Destruction of Records and Security Policies	Disclosure of Breaches
<p><b>CA</b> Cal Civ. Code § 1798.82 et seq.</p>	<p>For purposes of this section, “personal information” means an individual’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social Security number. (2) Driver’s license number or California Identification Card number. (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account.</p>	<p>Defined as “an unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information.”</p>	<p>Breach does not include good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business, provided no further use or unauthorized disclosure occurs.</p>		<p>Any person or business that conduct business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California 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 unreasonably delay, consistent with the legitimate needs of law enforcement, or any measures necessary to determine the scope of the breach and restore the reasonably integrity of the data system.</p> <p>Notification should be provided by: 1) Written notice; 2) Electronic notice consistent with 15 U.S.C. § 7001; or 3) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars (\$250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information.</p>

**STATE LAW: SECURITY BREACH NOTIFICATION**

State	“Personal Information”	“Breach”	Exceptions	Destruction of Records and Security Policies	Disclosure of Breaches
<p><b>CO</b></p> <p>COL. STAT § 6-1-716</p>	<p>Defined as a Colorado resident's first name or first initial and last name in combination with any one or more of the following data elements that relate to the resident, when the data elements are not encrypted, redacted, or secured by any other method rendering the name or the element unreadable or unusable: (A) SS number; (B) DL or ID card number; (C) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial account.</p>	<p>“Breach of the security of the system” means the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an individual or a commercial entity.</p>	<p>Good faith acquisition of personal information by an employee or agent of an individual or commercial entity for the purposes of the individual or commercial entity is not a breach of the security of the system if the personal information is not used for or is not subject to further unauthorized disclosure.</p>	<p>Each public and private entity in the state that uses documents during the course of business that contain personal identifying information shall develop a policy for the destruction or proper disposal of paper documents containing personal identifying information. (C.R.S.A. § 6-1-713)</p>	<p>When (an entity that conducts business in Colorado) 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.</p> <p>Notice shall be made in the most expedient time possible and without unreasonable delay.</p> <p>Notification should be provided by: (1) Written notice ; (2) Telephonic notice; (3) Electronic notice, consistent with 15 U.S.C. § 7001; or (4) Substitute notice, if the individual or the commercial entity required to provide notice demonstrates that the cost of providing notice will exceed two hundred fifty thousand dollars, the affected class of persons to be notified exceeds two hundred fifty thousand Colorado residents, or the individual or the commercial entity does not have sufficient contact information to provide notice.</p>

**STATE LAW: SECURITY BREACH NOTIFICATION**

State	“Personal Information”	“Breach”	Exceptions	Destruction of Records and Security Policies	Disclosure of Breaches
<p><b>CT</b> CGSA § 36a-701b</p>	<p>“Personal information” means an individual's first name or first initial and last name in combination with any one, or more, of the following data: (1) Social Security number; (2) driver's license number or state identification card number; or (3) account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account.</p>	<p>“Breach of security” 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.</p>			<p>Any person who conducts business in this state, and who, in the ordinary course of such person's business, owns, licenses or maintains computerized data that includes personal information, shall disclose any breach of security following the discovery of the breach to any resident of this state whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person through such breach of security. Such disclosure shall be made without unreasonable delay.</p> <p>Notification should be provided by: (1) Written notice; (2) Telephonic notice; (3) Electronic notice, consistent with 15 U.S.C. § 7001; or (4) Substitute notice, provided such person demonstrates that the cost of providing notice in accordance with subdivision (1), (2) or (3) of this subsection would exceed two hundred fifty thousand dollars, that the affected class of subject persons to be notified exceeds five hundred thousand persons or the person does not have sufficient contact information.</p>

**STATE LAW: SECURITY BREACH NOTIFICATION**

State	“Personal Information”	“Breach”	Exceptions	Destruction of Records and Security Policies	Disclosure of Breaches
<p><b>DE</b> DE ST TI 6 § 12B- 101 et seq.</p>	<p>Defined as an individual’s first name or first initial and last name in combination with any one or more of the following: (1) SS number; (2) DL or state ID number; (3) Account, credit, or debit card number in combination with any required security code, access code, or password that would permit access to the person’s financial account.</p>	<p>Defined as “unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information.”</p>	<p>Breach does not include good faith acquisition of personal information by an employee or agent of an individual or commercial entity for the purposes of the individual or commercial entity, provided that the personal information is not used or subject to further unauthorized disclosure.</p>		<p>Must be in the most expedient time possible and without unreasonable delay after law enforcement determines that notification will not impede investigation.</p> <p>Notification should be provided by: (1) Written notice; (2) Telephonic notice; (3) Electronic notice, consistent with 15 U.S.C. § 7001; or (4) Substitute notice, if the individual or the commercial entity required to provide notice demonstrates that the cost of providing notice will exceed \$75,000, or that the affected class of Delaware residents to be notified exceeds 100,000 residents, or that the individual or the commercial entity does not have sufficient contact information to provide notice.</p>

**STATE LAW: SECURITY BREACH NOTIFICATION**

State	“Personal Information”	“Breach”	Exceptions	Destruction of Records and Security Policies	Disclosure of Breaches
<p><b>DC</b>  DC ST Sec 28-3851 et seq.</p>	<p>Personal information" means:                      (i) An individual's first name or first initial and last name, or phone number, or address, and any one or more of the following data elements:                      (I) Social Security number;                      (II) Driver's license number or District of Columbia Identification Card number; or                      (III) Credit card number or debit card number; or                      (ii) Any other number or code or combination of numbers or codes, such as account number, security code, access code, or password, that allows access to or use of an individual's financial or credit account.</p>	<p>"Breach of the security of the system" means unauthorized acquisition of computerized or other electronic data, or any equipment or device storing such data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business.</p>	<p>"Breach of the security system" shall not include a good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business if the personal information is not used improperly or subject to further unauthorized disclosure. Acquisition of data that has been rendered secure, so as to be unusable by an unauthorized third party, shall not be deemed to be a breach of the security of the system.</p>		<p>Any person or entity who conducts business in the District of Columbia, and who, in the course of such business, owns or licenses computerized or other electronic data that includes personal information, and who discovers a breach of the security of the system, shall promptly notify any District of Columbia resident whose personal information was included in the breach. The notification shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.</p> <p>If any person or entity is required by this section to notify more than 1,000 persons of a breach of security, the person shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by section 603(p) of the Fair Credit Reporting Act.</p> <p>Notification should be provided by: (a) Written notice; (b) Electronic notice, consistent with 15 U.S.C. § 7001; or (c) Substitute notice, if the person or business demonstrates that the cost of providing notice to persons subject to this subchapter would exceed \$50,000, that the number of persons to receive notice under this subchapter exceeds 100,000, or that the person or business does not have sufficient contact information.</p>

**STATE LAW: SECURITY BREACH NOTIFICATION**

State	“Personal Information”	“Breach”	Exceptions	Destruction of Records and Security Policies	Disclosure of Breaches
<p><b>FL</b> F.S.A. § 817.5681</p>	<p>Defined as an individual’s first name, first initial and last name, or any middle name and last name in combination with any one or more of the following: (1) SS number; (2) DL or state ID number; (3) Account, credit, or debit card number in combination with any required security code, access code, or password that would permit access to the person’s financial account.</p>	<p>“Unlawful and unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the person.”</p>	<p>Breach does not include good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business, provided that the information is not used for a purpose unrelated to the business or subject to further unauthorized use.</p>		<p>Disclosure to any resident of this state whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person no later than 45 days following the determination of the breach.</p> <p>Notice should be provided by: 1) Written notice; 2) Electronic notice, if it is consistent with 15 U.S.C. § 7001 or if the person or business providing the notice has a valid email address for the subject person and the subject person has agreed to accept communications electronically; or 3) Substitute notice, if the person demonstrates that the cost of providing notice would exceed \$250,000, the affected class of subject persons to be notified exceeds 500,000, or the person does not have sufficient contact information.</p>

**STATE LAW: SECURITY BREACH NOTIFICATION**

State	“Personal Information”	“Breach”	Exceptions	Destruction of Records and Security Policies	Disclosure of Breaches
<p><b>GA</b> GA ST § 10-1-910 et seq.</p>	<p>Defined as a an individual’s first name or first initial and last name in combination with any one or more of the following: (1) SS number; (2) DL or state ID number; (3) Account, credit, or debit card number, if circumstances exist wherein such a number could be used without additional identifying information, access codes, or passwords (4) Account passwords PIN’s or other access codes (5) Any of the above items not in connection with names if the information compromised would be sufficient to perform or attempt to perform identity theft.</p>	<p>Defined as “unauthorized acquisition of an individuals computerized data that compromises the security, confidentiality or integrity of personal information.”</p>	<p>Breach does not include good faith acquisition of personal information by an employee or agent of an information broker for the purposes of such information broker, provided no further use or unauthorized disclosure occurs.</p>		<p>Any information broker or data collector that maintains computerized data that includes personal information of individuals shall give notice of any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The notice shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.</p> <p>Notice can be in writing or by electronic notice consistent with 15 U.S.C. § 7001.</p> <p>In the event that an information broker or data collector discovers circumstances requiring notification pursuant to this Code section of more than 10,000 residents of this state at one time, the information broker or data collector shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nation-wide basis, as defined by 15 U.S.C. Section 1681a, of the timing, distribution, and content of the notices.</p>

**STATE LAW: SECURITY BREACH NOTIFICATION**

State	“Personal Information”	“Breach”	Exceptions	Destruction of Records and Security Policies	Disclosure of Breaches
<p><b>HI</b> HRS § 487N-1 et seq.</p>	<p>“Personal information” means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social security number; (2) Driver's license number or Hawaii identification card number; or (3) Account number, credit or debit card number, access code, or password that would permit access to an individual's financial account.</p>	<p>“Security breach” means an incident of 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 that creates a risk of harm to a person. Any incident of unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential process or key constitutes a security breach.</p>	<p>Good faith acquisition of personal information by an employee or agent of the business for a legitimate purpose is not a security breach; provided that the personal information is not used for a purpose other than a lawful purpose of the business and is not subject to further unauthorized disclosure.</p>	<p>Any business or government agency that conducts business in Hawaii and any business or government agency that maintains or otherwise possesses personal information of a resident of Hawaii shall take reasonable measures to protect against unauthorized access to or use of the information in connection with or after its disposal. The reasonable measures shall include: (1) Implementing and monitoring compliance with policies and procedures that require the burning, pulverizing, recycling, or shredding of papers containing personal information so that information cannot be practicably read or reconstructed;</p>	<p>Any business that owns or licenses personal information of residents of Hawaii or any government agency that collects personal information for specific government purposes shall provide notice to the affected person that there has been a security breach following discovery or notification of the breach.</p> <p>Notice shall be made “without unreasonable delay” consistent with both law enforcement needs the need to determine the scope of the breach and ensure the integrity, security and confidentiality of the data.</p> <p>Notice can be (1) written; (2) telephonic; or (3) electronic consistent with 15 U.S.C. § 7001. If the cost of providing notice exceeds \$100,000 or over 200,000 people must be notified, notice can be made by email, posting the notice on the breaching party’s website, and notifying statewide media.</p> <p>The notice shall be clear and conspicuous. The notice shall include a description of the following: (1) The incident in general terms; (2) The type of personal information that was subject to the unauthorized access and acquisition; (3) The general acts of the business or government agency to protect the personal information from further unauthorized access; (4) A telephone number that the person may call for further information and assistance, if one exists;</p>

**STATE LAW: SECURITY BREACH NOTIFICATION**

State	“Personal Information”	“Breach”	Exceptions	Destruction of Records and Security Policies	Disclosure of Breaches
<p><b>HI</b>  Cont’d</p>				<p>(2) Implementing and monitoring compliance with policies and procedures that require the destruction or erasure of electronic media and other nonpaper media containing personal information so that the information cannot practicably be read or reconstructed; and (3) Describing procedures relating to the adequate destruction or proper disposal of personal records as official policy in the writings of the business entity. (HI ST § 487R-2 )</p>	<p>(5) Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit and reports.</p>

**STATE LAW: SECURITY BREACH NOTIFICATION**

<b>State</b>	<b>“Personal Information”</b>	<b>“Breach”</b>	<b>Exceptions</b>	<b>Destruction of Records and Security Policies</b>	<b>Disclosure of Breaches</b>
<p><b>ID</b> ID ST § 28-51-104 et seq.</p>	<p>“Personal information” means an Idaho resident's first name or first initial and last name in combination with any one (1) or more of the following data elements that relate to the resident, when either the name or the data elements are not encrypted: (a) Social Security number; (b) Driver's license number or Idaho identification card number; or (c) Account number, or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial account.</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>Good faith acquisition of personal information by an employee or agent of an agency, individual or a commercial entity for the purposes of the agency, individual or the commercial entity is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.</p>		<p>A commercial entity that conducts business in 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 commercial entity shall give notice in the most expedient time possible.</p> <p>Notification should be provided by: 1) Written notice; 2) Telephonic notice; 3) Electronic notice; or 4) Substitute notice, if the agency, individual or the commercial entity required to provide notice demonstrates that the cost of providing notice will exceed twenty-five thousand dollars (\$25,000), or that the number of Idaho residents to be notified exceeds fifty thousand (50,000), or that the agency, individual or the commercial entity does not have sufficient contact information to provide notice.</p>

**STATE LAW: SECURITY BREACH NOTIFICATION**

State	“Personal Information”	“Breach”	Exceptions	Destruction of Records and Security Policies	Disclosure of Breaches
<p><b>IL</b> 815 Ill. Comp. Stat. § 530/5 and 530/10</p>	<p>Defined as an individual’s first name, first initial and last name in combination with any one or more of the following: (1) SS number; (2) DL or state ID number; (3) Account, credit, or debit card number in combination with any required security code, access code, or password that would permit access to the person’s financial account.</p>	<p>Defined as “unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal information.”</p>	<p>Breach does not include good faith acquisition of personal information by an employee or agent of the data collector for a legitimate purpose, provided that the personal information is not used or subject to further unauthorized disclosure.</p>	<p>Any State agency that collects personal data that is no longer needed or stored at the agency shall dispose of the personal data or written material it has collected in such a manner as to ensure the security and confidentiality of the material. (815 ILCS 530/30)</p>	<p>Any data collector that owns or licenses personal information concerning an Illinois resident shall notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach. The disclosure notification shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.</p> <p>Notification should be provided by: 1) Written notice; 2) Electronic notice, if consistent with 15 U.S.C. § 7001; or 3) Substitute notice, if the data collector 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 data collector does not have sufficient contact information</p>

**STATE LAW: SECURITY BREACH NOTIFICATION**

State	“Personal Information”	“Breach”	Exceptions	Destruction of Records and Security Policies	Disclosure of Breaches
<p><b>IN</b> Ind. Code § 24-4.9</p>	<p>“Personal information” means: (1) a Social Security number that is not encrypted or redacted; or (2) an individual's first and last names, or first initial and last name, and one (1) or more of the following data elements that are not encrypted or redacted: (A) A driver's license number. (B) A state identification card number. (C) A credit card number. (D) A financial account number or debit card number in combination with a security code, password, or access code that would permit access to the person's account.</p>	<p>“Breach of the security of a system” means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person. The term includes the unauthorized acquisition of computerized data that have been transferred to another medium, including paper, microfilm, or a similar medium, even if the transferred data are no longer in a computerized format.</p>	<p>“Breach” does not include: (1) Good faith acquisition of personal information by an employee or agent of the person for lawful purposes of the person, if the personal information is not used or subject to further unauthorized disclosure. (2) Unauthorized acquisition of a portable electronic device on which personal information is stored, if access to the device is protected by a password that has not been disclosed.</p>	<p>A person who disposes of the unencrypted, unredacted personal information of a customer without shredding, incinerating, mutilating, erasing, or otherwise rendering the information illegible or unusable commits a Class C infraction. (IN ST 24-4-14-8)</p>	<p>After discovering or being notified of a breach of the security of a system, the data base owner shall disclose the breach to an Indiana resident whose: (1) unencrypted personal information was or may have been acquired by an unauthorized person or (2) encrypted personal information was or may have been acquired by an unauthorized person with access to the encryption key; if the data base owner knows, should know, or should have known that the unauthorized acquisition constituting the breach has resulted in or could result in identity deception (as defined in IC 35-43-5-3.5), identity theft, or fraud affecting the Indiana resident.</p> <p>Notice must be made “without reasonable delay” and can be by 1). Mail; 2). Telephone; 3). Fax; or 4). Email.</p>

**STATE LAW: SECURITY BREACH NOTIFICATION**

State	“Personal Information”	“Breach”	Exceptions	Destruction of Records and Security Policies	Disclosure of Breaches
<p><b>KS</b> Kan. Stat. Ann. 50-7a02 et seq.</p>	<p>“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 elements are neither encrypted nor redacted:                      (1) Social Security number;                      (2) Driver's license number or state identification card number; or                      (3) Financial account number, or credit or debit card number, alone or in combination with any required security code, access code or password that would permit access to a consumer's financial account.</p>	<p>“Security breach” means the unauthorized access and acquisition of unencrypted or unredacted computerized data that compromises the security, confidentiality or integrity of personal information maintained by an individual or a commercial entity and that causes, or such individual or entity reasonably believes has caused or will cause, identity theft to any consumer.</p>	<p>Good faith acquisition of personal information by an employee or agent of an individual or a commercial entity for the purposes of the individual or the commercial entity is not a breach of the security of the system, provided that the personal information is not used for or is not subject to further unauthorized disclosure.</p>	<p>Unless otherwise required by federal law or regulation, a person or business shall take reasonable steps to destroy or arrange for the destruction of a customer's records within its custody or control containing personal information which is no longer to be retained by the person or business by shredding, erasing or otherwise modifying the personal information in the records to make it unreadable or undecipherable through any means.</p>	<p>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 information has occurred or is reasonably likely to occur, the person... shall give notice as soon as possible to the affected Kansas resident. Notice must be made in the most expedient time possible and without unreasonable delay.</p> <p>Notice should be in writing or by electronic notice consistent with 15 U.S.C. § 7001. In the event that a person discovers circumstances requiring notification pursuant to this section of more than 1,000 consumers at one time, the person shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by <u>15 U.S.C. § 1681a(p)</u>, of the timing, distribution and content of the notices</p>

**STATE LAW: SECURITY BREACH NOTIFICATION**

State	“Personal Information”	“Breach”	Exceptions	Destruction of Records and Security Policies	Disclosure of Breaches
<p><b>LA</b> LA ST § 51:3071 et seq.</p>	<p>Defined as an individual’s first name, first initial and last name in combination with any one or more of the following: (1) SS number; (2) DL number; (3) Account, credit, or debit card number in combination with any required security code, access code, or password that would permit access to the person’s financial account.</p>	<p>Defined as, “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.”</p>	<p>Breach does not include good faith acquisition of personal information by an employee or agent of an agency or person for the purposes of the agency or person, provided no further use or unauthorized disclosure occurs.</p>		<p>Disclosure to any state resident “whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person.”</p> <p>Must be made in the most expedient time possible and without unreasonable delay consistent with the legitimate needs of law enforcement.</p> <p>Notice should provided by 1) Written notice; 2) Electronic notice consistent with 15 U.S.C. § 7001, by e-mail when the agency or person has an e-mail address for the subject persons; or 3) Substitute notification, if an agency or person demonstrates that the cost of providing notification would exceed two hundred fifty thousand dollars, or that the affected class of persons to be notified exceeds five hundred thousand, or the agency or person does not have sufficient contact information.</p>

**STATE LAW: SECURITY BREACH NOTIFICATION**

State	“Personal Information”	“Breach”	Exceptions	Destruction of Records and Security Policies	Disclosure of Breaches
<p><b>ME</b></p> <p>Me. Rev. Stat. Ann. tit. 10 § 1346 et seq.</p> <p>Amendments (highlighted) effective 12/31/07.</p>	<p>Defined as a an individual’s first name or first initial and last name in combination with any one or more of the following: (1) SS number; (2) DL or state ID number; (3) Account, credit, or debit card number, if circumstances exist wherein such a number could be used without additional identifying information, access codes, or passwords (4) Account passwords PIN’s or other access codes (5) Any of the above items not in connection with names if the information compromised would be sufficient to permit a person to fraudulently assume, or attempt to assume, the identity of the person whose information was compromised.</p>	<p>“Breach of the security of the system” or “security breach” means unauthorized acquisition of an individual’s computerized data that compromises the security, confidentiality or integrity of personal information of the individual maintained by a <b>person</b>.</p>	<p>Good faith acquisition of personal information by an employee or agent of a <b>person on behalf of the person</b> is not a breach of the security of the system if the personal information is not used for or subject to further unauthorized disclosure.</p>		<p><b>If an information broker that maintains computerized data that includes personal information becomes aware of a breach of the security of the system, the information broker shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused and shall give notice of a breach of the security of the system following discovery or notification of the security breach to a resident of this State whose personal information has been, or is reasonably believed to have been, acquired by an unauthorized person.</b></p> <p><b>If any other person who maintains computerized data that includes personal information becomes aware of a breach of the security of the system, the person shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused and shall give notice of a breach of the security of the system following discovery or notification of the security breach to a resident of this State if misuse of the personal information has occurred or if it is reasonably possible that misuse will occur.</b></p> <p>Notice must be by the most expeditious means possible. It should be written, electronic or by substitute notice if the person maintaining personal information demonstrates that the cost of providing notice would exceed \$5,000, that the affected class of individuals to be notified exceeds 1,000 or that the person maintaining personal information does not have sufficient contact information to provide written or electronic notice to those individuals.</p>

**STATE LAW: SECURITY BREACH NOTIFICATION**

State	“Personal Information”	“Breach”	Exceptions	Destruction of Records and Security Policies	Disclosure of Breaches
<p><b>MA</b></p> <p>Public Law 82-2007</p> <p>Effective February 3, 2008</p>	<p>“Personal information” means a Massachusetts resident’s first name or first initial and last name in combination with any one or more of the following data elements that relate to the resident, when either the name or the data elements are not encrypted: a. SS number; b. Driver’s license number or ID number; c. Account number, or credit or debit card number in combination with any required security code, access code, or password that would permit access to a resident’s financial account.</p>	<p>“Breach of security of the system” means the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an individual or a commercial entity.</p>	<p>Good-faith acquisition of personal information by an employee or agent of an individual or a commercial entity for the purposes of the individual or the commercial entity is not a breach of the security of the system, provided that the personal information is not used or subject for further unauthorized disclosure.</p>		<p>An individual or a commercial entity that conducts business in Massachusetts and that owns or licenses computerized data that includes personal information about a resident of Massachusetts shall, when it becomes aware of a breach of the security of the system, conduct in good faith a reasonably 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 a resident has occurred or is reasonably likely to occur, the individual or the commercial entity shall give notice as soon as possible to the affected resident. Notice must be made in the most effective and 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.</p> <p>Notification should be in writing, by telephone, by electronic notice consistent with 15 U.S.C. § 7001, or by substitute notice if the individual or the commercial entity required to provide notice demonstrates that the cost of providing notice will exceed \$250,000, or that the affected class of residents notified exceeds 500,000 residents, or that the individual or the commercial entity does not have sufficient contact information to provide notice.</p>

**STATE LAW: SECURITY BREACH NOTIFICATION**

State	“Personal Information”	“Breach”	Exceptions	Destruction of Records and Security Policies	Disclosure of Breaches
<p><b>MI</b>  Mich. Pub. Act No. 566</p>	<p>Defined as an individual’s first name, first initial and last name in combination with any one or more of the following for residents of Michigan: (1) SS number; (2) DL or state ID number; (3) Demand deposit or other financial account, credit, or debit card number in combination with any required security code, access code, or password that would permit access to the resident’s financial account.</p>	<p>“Breach of the security of a database” or “security breach” means unauthorized access and acquisition of data that compromises the security or confidentiality of personal information maintained by a person or agency as part of a database of personal information regarding multiple individuals.</p>	<p>Breach does not include good faith acquisition of personal information by an employee or person for use in the activities of the agency or person, provided no further use or unauthorized disclosure occurs.</p>		<p>Disclosure to each state resident whose “unencrypted and unredacted personal information was accessed and acquired by an unauthorized person” or whose “personal information was accessed and acquired in encrypted form by a person with unauthorized access to the encryption key”</p> <p>Notice must be made “without unreasonable delay,” except to learn the scope of the breach, to ensure the integrity of the database or for law enforcement purposes.</p> <p>Notice should be in writing, or if certain conditions are met, by email or telephone. If the cost of providing notice will exceed \$250,000 or must be provided to more than 500,000 residents, the notice can be given through the combined means of notifying statewide media, posting on the business’s website, and email notice.</p>

**STATE LAW: SECURITY BREACH NOTIFICATION**

State	“Personal Information”	“Breach”	Exceptions	Destruction of Records and Security Policies	Disclosure of Breaches
<p><b>MN</b> MN ST § 325E.61</p>	<p>Defined as an individual’s first name, first initial and last name in combination with any one or more of the following: (1) SS number; (2) DL or state ID number; (3) Account, credit, or debit card number in combination with any required security code, access code, or password that would permit access to an individual’s financial account.</p>	<p>Defined as “unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal information.”</p>	<p>Breach does not include good faith acquisition of personal information by an employee or agent of the business or person for the purposes of the business or person, provided no further use or unauthorized disclosure occurs.</p>		<p>Any person or business that conducts business in this state, and that owns or licenses data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or with any measures necessary to determine the scope of the breach, identify the individuals affected, and restore the reasonable integrity of the data system.</p> <p>Notification should be in writing, by electronic notice, consistent with 15 U.S.C. § 7001, or by substitute notice, if the person or 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 person or business does not have sufficient contact information.</p>

**STATE LAW: SECURITY BREACH NOTIFICATION**

<b>State</b>	<b>“Personal Information”</b>	<b>“Breach”</b>	<b>Exceptions</b>	<b>Destruction of Records and Security Policies</b>	<b>Disclosure of Breaches</b>
<p><b>MT</b> Mont. Code Ann. § 31-3-115</p>	<p>Defined as an individual’s first name, first initial and last name in combination with any one or more of the following: (1) SS number; (2) DL or state ID number; (3) Account, credit, or debit card number in combination with any required security code, access code, or password that would permit access to an individual’s financial account.</p>	<p>Defined as “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 Montana resident.”</p>	<p>Breach does not include good faith acquisition of personal information by an employee or agent of the business or person for the purposes of the business or person, provided no further use or unauthorized disclosure occurs.</p>	<p>Must take “all reasonable steps” to destroy customer records which are no longer to be retained by shredding, erasing, or otherwise making it unreadable or undecipherable.</p>	<p>Disclosure to any state resident “whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.”</p> <p>Must be by most expedient means and without unreasonable delay consistent with the legitimate needs of law enforcement.</p> <p>Notice can be (1) written; (2) electronic consistent with 15 U.S.C. § 7001; or (3) telephonic.</p>

**STATE LAW: SECURITY BREACH NOTIFICATION**

State	“Personal Information”	“Breach”	Exceptions	Destruction of Records and Security Policies	Disclosure of Breaches
<p><b>NE</b> Neb. Rev. Stat. § 87-801 et seq. 2006 LB 876</p>	<p>Defined as a first name or first initial and last name in combination with any one or more of the following data elements that relate to the resident if either the name or the data elements are not encrypted, redacted, or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable: (a) SS number; (b) Driver’s license number or state ID number; (c) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a resident’s financial account; (d) Unique electronic identification number or routing code, in combination with any required security code, access code, or password; or (e) Unique biometric data, such as a fingerprint, voice print, or retina or iris image, or other unique physical representation.</p>	<p>Breach of the security of the system means the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an individual or a commercial entity.</p>	<p>Good faith acquisition of personal information by an employee or agent of an individual or a commercial entity for the purposes of the individual or the commercial entity is not a breach of the security of the system if the personal information is not used or subject to further unauthorized disclosure. Acquisition of personal information pursuant to a search warrant, subpoena, or other court order or pursuant to a subpoena or order of a state agency is not a breach of the security of the system.</p>		<p>An individual or a commercial entity that conducts business in Nebraska and that owns or licenses computerized data that includes personal information about a resident of Nebraska 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 used for an unauthorized purpose. If the investigation determines that the use of information about a Nebraska resident for an unauthorized purpose has occurred or is reasonably likely to occur, the individual or commercial entity shall give notice to the affected Nebraska resident. Notice shall be made as soon as possible and without unreasonable delay.</p> <p>Notification should be provided by: 1) Written notice; 2) Telephonic notice; 3) Electronic notice, consistent with 15 U.S.C. § 7001; or 4) Substitute notice, if the individual or commercial entity required to provide notice demonstrates that the cost of providing notice will exceed seventy-five thousand dollars, that the affected class of Nebraska residents to be notified exceeds one hundred thousand residents, or that the individual or commercial entity does not have sufficient contact information to provide notice.</p>

**STATE LAW: SECURITY BREACH NOTIFICATION**

State	“Personal Information”	“Breach”	Exceptions	Destruction of Records and Security Policies	Disclosure of Breaches
<p><b>NV</b> Nev. Rev. Stat. 603A.200 et seq.</p>	<p>Defined as an individual’s first name, first initial and last name in combination with any one or more of the following: (1) SS number; (2) DL or state ID number; (3) Account, credit, or debit card number in combination with any required security code, access code, or password that would permit access to an individual’s financial account.</p>	<p>Defined as “unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information maintained by the data collector.”</p>	<p>Breach does not include good faith acquisition of personal information by an employee or agent of the data collector for the purposes of the data collector, provided no further use or unauthorized disclosure occurs.</p>	<p>A business that maintains records which contain personal information concerning the customers of the business shall take reasonable measures to ensure the destruction of those records when the business decides that it will no longer maintain the records. This includes: (1) Shredding of the record containing the personal information; or (2) Erasing of the personal information from the records.</p>	<p>Any data collector that owns or licenses computerized data which includes personal information shall disclose any breach of the security of the system data following discovery or notification of the breach to any resident of this State whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.</p> <p>Must be by most expedient means and without unreasonable delay consistent with the legitimate needs of law enforcement.</p> <p>Notice can be in writing or by electronic notice consistent with 15 U.S.C. § 7001.</p>

**STATE LAW: SECURITY BREACH NOTIFICATION**

State	“Personal Information”	“Breach”	Exceptions	Destruction of Records and Security Policies	Disclosure of Breaches
<p><b>NH</b> HB 1660  N.H. Rev. Stat. § 359-c:19 et seq.</p>	<p>“Personal information” means an individual’s first name or initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social Security number. (2) Driver’s license number or other government identification number. (3) Account number, credit card number, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account.</p>	<p>“Security breach” means unauthorized acquisition of computerized data that compromises the security or confidentiality of personal information maintained by a person doing business in this state.</p>	<p>Good faith acquisition of personal information by an employee or agent of a person for the purposes of the person’s business shall not be considered a security breach, provided that the personal information is not used or subject to further unauthorized disclosure.</p>		<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.</p> <p>Notification should be provided by: 1) Written notice; 2) Electronic notice; 3) Telephonic notice; or 4) Substitute notice if the person demonstrates that the cost of providing notice would exceed \$5,000, that the affected class of subject individuals to be notified exceeds 1,000, or the person does not have sufficient contact information.</p> <p>Notice under this section shall include at a minimum: (a) A description of the incident in general terms. (b) The approximate date of breach. (c) The type of personal information obtained as a result of the security breach. (d) The telephonic contact information of the person subject to this section.</p>

**STATE LAW: SECURITY BREACH NOTIFICATION**

State	“Personal Information”	“Breach”	Exceptions	Destruction of Records and Security Policies	Disclosure of Breaches
<p><b>NJ</b></p> <p>NJ ST 56:8-161 et seq.</p>	<p>“Personal information” means an individual's first name or first initial and last name linked with any one or more of the following data elements: (1) Social Security number; (2) driver's license number or State identification card number; or (3) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. Dissociated data that, if linked, would constitute personal information is personal information if the means to link the dissociated data were accessed in connection with access to the dissociated data.</p>	<p>“Breach of security” 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 or technology that renders the personal information unreadable or unusable.</p>	<p>Good faith acquisition of personal information by an employee or agent of the business for a legitimate business purpose is not a breach of security, provided that the personal information is not used for a purpose unrelated to the business or subject to further unauthorized disclosure.</p>	<p>A business or public entity shall destroy, or arrange for the destruction of, a customer's records within its custody or control containing personal information, which is no longer to be retained by the business or public entity, by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable, undecipherable or nonreconstructable through generally available means.</p>	<p>Any business that conducts business in New Jersey, or any public entity that compiles or maintains computerized records that include personal information, shall disclose any breach of security of those computerized records following discovery or notification of the breach to any customer who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person. The disclosure to a customer shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. Disclosure of a breach of security to a customer shall not be required under this section if the business or public entity establishes that misuse of the information is not reasonably possible. Any determination shall be documented in writing and retained for five years.</p> <p>For purposes of this section, notice should be provided by one of the following methods: (1) Written notice; (2) Electronic notice, if the notice provided is consistent with (<a href="#">15 U.S.C. s.7001</a>); or (3) Substitute notice, if the business or public entity demonstrates that the cost of providing notice would exceed \$250,000, or that the affected class of subject persons to be notified exceeds 500,000, or the business or public entity does not have sufficient contact information.</p>

**STATE LAW: SECURITY BREACH NOTIFICATION**

State	“Personal Information”	“Breach”	Exceptions	Destruction of Records and Security Policies	Disclosure of Breaches
<p><b>NY</b></p> <p><b>NY General Business Law § 899-aa</b></p>	<p>(a) “Personal information” shall mean any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person;</p> <p>(b) "Private information" shall mean personal information consisting of any information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted, or encrypted with an encryption key that has also been acquired: (1) social security number; (2) driver's license number or non-driver identification</p>	<p>“Breach of the security of the system” shall mean unauthorized acquisition or acquisition without valid authorization of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a business.</p>	<p>Good faith acquisition of personal information by an employee or agent of the business for the purposes of the business is not a breach of the security of the system, provided that the private information is not used or subject to unauthorized disclosure.</p>		<p>Any person or business which conducts business in New York state, and which owns or licenses computerized data which includes private information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of New York state whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement.</p> <p>In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization, such business may consider the following factors, among others: (1) indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information; or (2) indications that the information has been downloaded or copied; or (3) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.</p> <p>The notice required by this section shall be directly provided to the affected persons by one of the following methods: (a) Written notice; (b) Electronic notice, provided that the person to</p>

**STATE LAW: SECURITY BREACH NOTIFICATION**

State	“Personal Information”	“Breach”	Exceptions	Destruction of Records and Security Policies	Disclosure of Breaches
<p><b>NY</b>  Cont’d</p>	<p>card number; or (3) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.</p>				<p>whom notice is required has expressly consented to receiving said notice in electronic form and a log of each such notification is kept by the person or business who notifies affected persons in such form; provided further, however, that in no case shall any person or business require a person to consent to accepting said notice in said form as a condition of establishing any business relationship or engaging in any transaction; (c) Telephone notification provided that a log of each such notification is kept by the person or business who notifies affected persons;’ or (d) Substitute notice, if a business demonstrates to the state attorney general that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or such business does not have sufficient contact information</p>

**STATE LAW: SECURITY BREACH NOTIFICATION**

State	“Personal Information”	“Breach”	Exceptions	Destruction of Records and Security Policies	Disclosure of Breaches
<p><b>NC</b> N.C.G.S. A. § 75-61 et seq.</p>	<p>A person's first name or first initial and last name in combination with identifying information: (1) Social Security or employer taxpayer identification numbers. (2) Drivers license, State identification card, or passport numbers. (3) Checking account numbers. (4) Savings account numbers. (5) Credit card numbers. (6) Debit card numbers. (7) Personal Identification (PIN) Code as defined in <a href="#">G.S. 14-113.8(6)</a>. (8) Electronic identification numbers, electronic mail names or addresses, Internet account numbers, or Internet identification names. (9) Digital signatures. (10) Any other numbers or information that can be used to access a</p>	<p>“Security breach”. -- An incident of unauthorized access to and acquisition of unencrypted and unredacted records or data containing personal information where illegal use of the personal information has occurred or is reasonably likely to occur or that creates a material risk of harm to a consumer. Any incident of unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential process or key shall constitute a security breach.</p>	<p>Good faith acquisition of personal information by an employee or agent of the business for a legitimate purpose is not a security breach, provided that the personal information is not used for a purpose other than a lawful purpose of the business and is not subject to further unauthorized disclosure.</p>	<p>Any business that conducts business in North Carolina and any business that maintains or otherwise possesses personal information of a resident of North Carolina must take reasonable measures to protect against unauthorized access to or use of the information in connection with or after its disposal. The reasonable measures must include: (1) Implementing and monitoring compliance with policies and procedures that require the burning, pulverizing, or shredding of papers containing personal information so that information cannot be practicably read or</p>	<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.</p> <p>The notice shall be clear and conspicuous. The notice shall include a description of the following: (1) The incident in general terms. (2) The type of personal information that was subject to the unauthorized access and acquisition. (3) The general acts of the business to protect the personal information from further unauthorized access. (4) A telephone number that the person may call for further information and assistance, if one exists. (5) Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports. For purposes of this section, notice to affected persons may be provided by one of the following methods: (1)</p>

**STATE LAW: SECURITY BREACH NOTIFICATION**

State	“Personal Information”	“Breach”	Exceptions	Destruction of Records and Security Policies	Disclosure of Breaches
<p><b>NC</b>  Cont’d</p>	<p>person's financial resources. (11) Biometric data. (12) Fingerprints. (13) Passwords. (14) Parent's legal surname prior to marriage.</p>			<p>reconstructed. (2) Implementing and monitoring compliance with policies and procedures that require the destruction or erasure of electronic media and other nonpaper media containing personal information so that the information cannot practicably be read or reconstructed. (3) Describing procedures relating to the adequate destruction or proper disposal of personal records as official policy in the writings of the business entity.</p>	<p>Written notice. (2) Electronic notice, for those persons for whom it has a valid e-mail address and who have agreed to receive communications electronically if the notice provided is consistent with the provisions regarding electronic records and signatures for notices legally required to be in writing set forth in 15 U.S.C. § 7001. (3) Telephonic notice provided that contact is made directly with the affected persons. (4) Substitute notice, if the business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars (\$250,000) or that the affected class of subject persons to be notified exceeds 500,000, or if the business does not have sufficient contact information or consent to satisfy subdivisions (1), (2), or (3) of this subsection, for only those affected persons without sufficient contact information or consent, or if the business is unable to identify particular affected persons, for only those unidentifiable affected persons.</p>

**STATE LAW: SECURITY BREACH NOTIFICATION**

State	“Personal Information”	“Breach”	Exceptions	Destruction of Records and Security Policies	Disclosure of Breaches
<p><b>ND</b> ND ST § 51-30-01 et seq.</p>	<p>Defined as an individual’s first name, first initial and last name in combination with any one or more of the following: (1) SS number; (2) DOT operator license number; (3) DOT color photo ID number; (4) Account, credit, or debit card number in combination with any required security code, access code, or password that would permit access to an individual’s financial account; (5) DOB; (6) Mother’s maiden name; (7) Employee ID number; (8) Digitized or electronic signature.</p>	<p>Defined as, “unauthorized acquisition of computerized data” when access has not been secured by encryption or other means.</p>	<p>Breach does not include good faith acquisition of personal information by an employee or agent of the person, provided no further use or unauthorized disclosure occurs.</p>		<p>Disclosure to any state resident “whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.”</p> <p>Must be in the most expedient time possible and without unreasonable delay consistent with the legitimate needs of law enforcement.</p> <p>Notification can be by written notice, electronic notice, consistent with 15 U.S.C. § 7001, or by substitute notice, if the person demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or the person does not have sufficient contact information.</p>

**STATE LAW: SECURITY BREACH NOTIFICATION**

State	“Personal Information”	“Breach”	Exceptions	Destruction of Records and Security Policies	Disclosure of Breaches
<p><b>OH</b> OH ST § 1349.19</p>	<p>“Personal information” means an individual's name, consisting of the individual's first name or first initial and last name, in combination with and linked to any one or more of the following data elements, when the data elements are not encrypted, redacted, or altered by any method or technology in such a manner that the data elements are unreadable: (i) Social Security number; (ii) Driver's license number or state identification card number; (iii) Account number or credit or debit card number, in combination with and linked to any required security code, access code, or password that would permit access to an individual's financial account.</p>	<p>“Breach of the security of the system” means unauthorized access to and acquisition of computerized data that compromises the security or confidentiality of personal information owned or licensed by a person and that causes, reasonably is believed to have caused, or reasonably is believed will cause a material risk of identity theft or other fraud to the person or property of a resident of this state.</p>	<p>Good faith acquisition of personal information by an employee or agent of the person for the purposes of the person is not a breach of the security of the system, provided that the personal information is not used for an unlawful purpose or subject to further unauthorized disclosure.</p> <p>Acquisition of personal information pursuant to a search warrant, subpoena, or other court order, or pursuant to a subpoena, order, or duty of a regulatory state agency, is not a breach of the security of the system.</p>		<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 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.</p> <p>Notification can be provided by: (1) Written notice; (2) Electronic notice, if the person's primary method of communication with the resident to whom the disclosure must be made is by electronic means; (3) Telephonic notice; or (4) Substitute notice in accordance with this division, if the person required to disclose demonstrates that the person does not have sufficient contact information to provide notice in a manner described in division (1), (2), or (3) of this section, or that the cost of providing disclosure or notice to residents to whom disclosure or notification is required would exceed two hundred fifty thousand dollars, or that the affected class of subject residents to whom disclosure or notification is required exceeds five hundred thousand persons.</p>

**STATE LAW: SECURITY BREACH NOTIFICATION**

State	“Personal Information”	“Breach”	Exceptions	Destruction of Records and Security Policies	Disclosure of Breaches
<p><b>OK</b></p> <p>Okla. Stat. tit. 74 § 3113.1</p> <p>(Applies only to State and Gov’t breaches)</p>	<p>Personal information is the first name or first initial and last name of an individual in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (a) SSN (b) Driver’s license number (c) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to the financial account of an individual.</p>	<p>Unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal information maintained by the state agency, board, commission or other unit or subdivision of state government.</p>	<p>Good faith acquisition of personal information by an employee or agent of the state government for the purposes of that entity is not a breach provided the information is not used or disclosed further.</p>		<p>Disclosure shall be made by the state agency, board, commission or other unit or subdivision of state government that owns or licenses data including personal information to the resident of Oklahoma whose unencrypted personal information was, or is reasonably believed to have been acquired by an unauthorized person.</p> <p>The disclosure shall be made in the most expedient time possible, and without unreasonable delay, consistent with the legitimate needs of law enforcement or measures necessary to determine the scope of the breach and to secure the integrity of the data.</p> <p>Notice can be in writing or by electronic notice consistent with 15 U.S.C. § 7001.</p> <p>Substitute notice can be made when the cost exceeds \$250,000 or more than 500,000 people must be notified. Substitute notice is made by email to the affected individuals, conspicuous posting on the agency’s website if one exists, and notification to major statewide media.</p>

**STATE LAW: SECURITY BREACH NOTIFICATION**

State	“Personal Information”	“Breach”	Exceptions	Destruction of Records and Security Policies	Disclosure of Breaches
<p><b>OR</b> SB 583 Effective October 1, 2007</p>	<p>“Personal information” means a consumer’s first name or first initial and last name in combination with any one or more of the following data elements, when the data elements are not rendered unusable through encryption, redaction or other methods, or when the data elements are encrypted and the encryption key has also been acquired: (a) SS number; (b) Driver license number or state ID number; (c) Passport number or other US ID number; (d) Financial account number credit or debit card number, in combination with any required security code, access code or password that would permit access to a consumer’s financial account.</p>	<p>“Breach of security” means unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information maintained by the person.</p>	<p>This does not include good-faith acquisition of personal information by a person or that person’s employee or agent for legitimate purpose of that person 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.</p>		<p>Any person that owns, maintains or otherwise possesses personal information on behalf of another person shall notify the owner or licensor of the information of any breach of security immediately following discovery of such breach of security if a consumer’s personal information was included in the information that was breached. The disclosure notification shall be made in the most expeditious time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine sufficient contact information for the consumers, determine the scope of the breach and restore the reasonably integrity, security and confidentiality of the data.</p> <p>Notification can be provided by written notice, electronic notice, telephonic notice or substitute notice, if the person demonstrates that the cost of providing notice would exceed \$250,000, that the affected class of consumers to be notified exceeds \$350,000, or if the person does not have sufficient contact information to provide notice.</p>

**STATE LAW: SECURITY BREACH NOTIFICATION**

State	“Personal Information”	“Breach”	Exceptions	Destruction of Records and Security Policies	Disclosure of Breaches
<p><b>PA</b> 73 PA ST § 2301 et seq.</p>	<p>“Personal information.” (1) An individual's first name or first initial and last name in combination with and linked to any one or more of the following data elements when the data elements are not encrypted or redacted: (i) Social Security number. (ii) Driver's license number or a State identification card number issued in lieu of a driver's license. (iii) Financial account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account.</p>	<p>“Breach of the security of the system.” The unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of personal information maintained by the entity as part of a database of personal information regarding multiple individuals and that causes or the entity reasonably believes has caused or will cause loss or injury to any resident of this Commonwealth.</p>	<p>Good faith acquisition of personal information by an employee or agent of the entity for the purposes of the entity is not a breach of the security of the system if the personal information is not used for a purpose other than the lawful purpose of the entity and is not subject to further unauthorized disclosure.</p>		<p>An entity that maintains, stores or manages computerized data that includes personal information shall provide notice of any breach of the security of the system following discovery of the breach of the security of the system to any resident of this Commonwealth whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person... the notice shall be made without unreasonable delay. “Notice.” May be provided by any of the following methods of notification: (1) Written notice to the last known home address for the individual. (2) Telephonic notice, if the customer can be reasonably expected to receive it and the notice is given in a clear and conspicuous manner, describes the incident in general terms and verifies personal information but does not require the customer to provide personal information and the customer is provided with a telephone number to call or Internet website to visit for further information or assistance. (3) E-mail notice, if a prior business relationship exists and the person or entity has a valid e-mail address for the individual. 4) Substitute notice, if the entity demonstrates one of the following: (A) The cost of providing notice would exceed \$100,000. (B) The affected class of subject persons to be notified exceeds 175,000. (C) The entity does not have sufficient contact information.</p>

**STATE LAW: SECURITY BREACH NOTIFICATION**

State	“Personal Information”	“Breach”	Exceptions	Destruction of Records and Security Policies	Disclosure of Breaches
<p><b>RI</b> RI ST § 11-49.2-1 et seq.</p>	<p>Defined as an individual’s first name, first initial and last name in combination with any one or more of the following: (1) SS number; (2) DL or state ID number; (3) Account, credit, or debit card number in combination with any required security code, access code, or password that would permit access to an individual’s financial account.</p>	<p>Defined as “unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality or integrity of personal information.”</p>	<p>Breach does not include good faith acquisition of personal information by an employee or agent of the agency, for the purposes of the agency, provided no further use or unauthorized disclosure occurs.</p>	<p>Must implement and maintain “reasonable security procedures and practices” to protect personal information from unauthorized access, destruction, use, modification, or disclosure.</p>	<p>Disclosure to any state resident “whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person or a person without authority.”</p> <p>Must be in the most expedient time possible and without unreasonable delay consistent with the legitimate needs of law enforcement.</p> <p>Notification should be provided by written notice, electronic notice, consistent with 15 U.S.C. § 7001, or substitute notice, if the state agency or person demonstrates that the cost of providing notice would exceed twenty-five thousand dollars (\$25,000), or that the affected class of subject persons to be notified exceeds fifty thousand (50,000), or the state agency or person does not have sufficient contact information.</p>

**STATE LAW: SECURITY BREACH NOTIFICATION**

State	“Personal Information”	“Breach”	Exceptions	Destruction of Records and Security Policies	Disclosure of Breaches
<p><b>TN</b> T.C.A. § 47-18-2107</p>	<p>Defined as an individual’s first name, first initial and last name in combination with any one or more of the following: (1) SS number; (2) DL number; (3) Account, credit, or debit card number in combination with any required security code, access code, or password that would permit access to an individual’s financial account.</p>	<p>Defined as “unauthorized acquisition of unencrypted computerized data that materially compromises the security, confidentiality or integrity of personal information.”</p>	<p>Breach does not include good faith acquisition of personal information by an employee or agent of the information holder, provided no further use or unauthorized disclosure occurs.</p>		<p>Disclosure to any state resident “whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.”</p> <p>Must be in the most expedient time possible and without unreasonable delay consistent with the legitimate needs of law enforcement.</p> <p>Notification can be provided by: 1) Written notice; 2) Electronic notice, consistent with 15 U.S.C. § 7001; or 3) Substitute notice, if the information holder demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars (\$250,000), or that the affected class of subject persons to be notified exceeds five hundred thousand (500,000), or the information holder does not have sufficient contact information.</p>

**STATE LAW: SECURITY BREACH NOTIFICATION**

State	“Personal Information”	“Breach”	Exceptions	Destruction of Records and Security Policies	Disclosure of Breaches
<p><b>TX</b></p> <p>TX Bus &amp; Com § 48.002 and 48.102 et seq.</p>	<p>Texas defines sensitive personal information as an individual’s first name, first initial and last name in combination with any one or more of the following: (1) SS number; (2) DL number or government issued ID number; (3) Account, credit, or debit card number in combination with any required security code, access code, or password that would permit access to an individual’s financial account.</p>	<p>Defined as “unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality or integrity of sensitive personal information.”</p>	<p>Breach does not include good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person, provided no further use or unauthorized disclosure occurs.</p>	<p>Must destroy customer records containing sensitive personal information that are no longer to be retained by shredding, erasing, or making it unreadable by any means.</p> <p>Must maintain and implement reasonable security procedures to protect and safeguard from unlawful use or disclosure.</p>	<p>Disclosure to any state resident “whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.”</p> <p>Must be as quickly as possible and consistent with the needs of law enforcement.</p> <p>Notification can be provided by: (a) Written notice; (b) Electronic notice, consistent with 15 U.S.C. § 7001; or (c) If the person or business demonstrates that the cost of providing notice would exceed \$250,000, the number of affected persons exceeds 500,000, or the person does not have sufficient contact information, the notice may be given by: (1) Electronic mail, if the person has an electronic mail address for the affected persons; (2) Conspicuous posting of the notice on the person's website; or (3) Notice published in or broadcast on major statewide media.</p>

**STATE LAW: SECURITY BREACH NOTIFICATION**

State	“Personal Information”	“Breach”	Exceptions	Destruction of Records and Security Policies	Disclosure of Breaches
<p><b>UT</b></p> <p>Utah Code Ann. § 13-44-101 et seq.</p>	<p>“Personal information” means a person's first name or first initial and last name, combined with any one or more of the following data elements relating to that person when either the name or date element is unencrypted or not protected by another method that renders the data unreadable or unusable:</p> <p>(i) Social Security number;</p> <p>(ii)(A) Financial account number, or credit or debit card number; and (B) Any required security code, access code, or password that would permit access to the person's account; or (iii) Driver's license number or state identification card number.</p>	<p>“Breach of system security” means an unauthorized acquisition of computerized data maintained by a person that compromises the security, confidentiality, or integrity of personal information.</p>	<p>“Breach of system security” does not include the acquisition of personal information by an employee or agent of the person possessing unencrypted computerized data unless the personal information is used for an unlawful purpose or disclosed in an unauthorized manner.</p>	<p>Any person who conducts business in the state and maintains personal information shall implement and maintain reasonable procedures to: (a) Prevent unlawful use or disclosure of personal information collected or maintained in the regular course of business; and (b) Destroy, or arrange for the destruction of, records containing personal information that are not to be retained by the person. (2) The destruction of records under Subsection (1)(b) shall be by: (a) Shredding; (b) Erasing; or (c) Otherwise modifying the personal information to make the information indecipherable.</p>	<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>(b) If an investigation under Subsection (1)(a) 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.</p> <p>A notification required by this section may be provided: (i) In writing by first-class mail to the most recent address the person has for the resident; (ii) Electronically, if the person's primary method of communication with the resident is by electronic means, or if provided in accordance with the consumer disclosure provisions of 15 U.S.C. Section 7001; (iii) By telephone, including through the use of automatic dialing technology not prohibited by other law; or (iv) By publishing notice of the breach of system security in a newspaper of general circulation.</p>

**STATE LAW: SECURITY BREACH NOTIFICATION**

State	“Personal Information”	“Breach”	Exceptions	Destruction of Records and Security Policies	Disclosure of Breaches
<p><b>VT</b> Vt. Stat. Ann. Tit. 9 § 2430 et seq.</p>	<p>Defined as an individual’s first name, first initial and last name in combination with any one or more of the following (if not encrypted, redacted, or protected by another method that renders them unreadable or unusable by unauthorized persons): (1) SS number; (2) license or state ID number; (3) Financial account, credit, or debit card number that can be used without additional identifying information, access codes, or passwords, account passwords or personal identification numbers or other access codes for a financial account.</p>	<p>Unauthorized acquisition or access of computerized data that compromises the security, confidentiality or integrity of personal information maintained by the data collector.</p>	<p>Good faith but unauthorized acquisition or access of personal information by an employee or agent of the data collector for a legitimate purpose of the data collector, provided that the personal information is not used for a purpose unrelated to the data collector’s business or subject to further unauthorized disclosure.</p>	<p>A business shall take all reasonable steps to destroy or arrange for the destruction of a customer’s records within its custody or control containing personal information which is no longer to be retained by the business by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable or indecipherable through any means for the purpose of: (1) Ensuring the security and confidentiality of customer personal information; (2) Protecting against any anticipated threats or hazards to the security or integrity of customer personal information; and (3) Protecting against unauthorized access to or use of customer personal information.</p>	<p>Breaches must be disclosed in the most expedient time possible and without unreasonable delay, consistent with the needs of law enforcement or with measures necessary to determine the scope of the breach and to restore the reasonable integrity, security and confidentiality of the data system.</p> <p>Notice may be in writing, electronic (if certain conditions are met), or by direct telephone contact.</p> <p>Substitute notice is allowed if the cost to notify customers exceeds \$5,000 or if the number of customers involved exceeds 5,000. Substitute notice is posting on the data collector’s website if they have one and notification of major statewide and regional media.</p>

**STATE LAW: SECURITY BREACH NOTIFICATION**

State	“Personal Information”	“Breach”	Exceptions	Destruction of Records and Security Policies	Disclosure of Breaches
<p><b>WA</b> Wash. Rev. Code § 19.255.010 et seq.</p>	<p>Defined as an individual’s first name, first initial and last name in combination with any one or more of the following: (1) SS number; (2) DL or state ID number; (3) Account, credit, or debit card number in combination with any required security code, access code, or password that would permit access to an individual’s financial account.</p>	<p>Defined as “unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information.”</p>	<p>Breach does not include good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business, provided no further use or unauthorized disclosure occurs.</p>		<p>Disclosure to any state resident “whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.”</p> <p>Must be in the most expedient time possible and without unreasonable delay consistent with the legitimate needs of law enforcement.</p> <p>Notification can be by: 1) Written notice; 2) Electronic notice, consistent with 15 U.S.C. § 7001; or 3) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or the person or business does not have sufficient contact information.</p>

**STATE LAW: SECURITY BREACH NOTIFICATION**

State	“Personal Information”	“Breach”	Exceptions	Destruction of Records and Security Policies	Disclosure of Breaches
<p><b>WI</b>  Wis. Stat. § 895.507</p>	<p>Defined as 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. SS number. 2. Driver's license number or state identification number. 3. Financial account number, including a credit or debit card account number, or any security code, access code, or password that would permit access to the individual's financial account. 4. The individual's deoxyribonucleic acid profile, as defined in s. 939.74(2d)(a). 5. The individual's unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation.</p>	<p>(a) If an entity whose principal place of business is <u>located in this state</u> or an entity that maintains or licenses personal information in this state knows that personal information in the entity's possession has been acquired by a person whom the entity has not authorized to acquire the personal information, (b) If an entity whose principal place of business is <u>not located in this state</u> knows that personal information pertaining to a <u>resident of this state</u> has been acquired by a person whom the entity has not authorized to acquire the personal information, (There is a separate rule for data storage companies.)</p>	<p>An entity is not required to provide notice of the acquisition of personal information if any of the following applies:</p> <ol style="list-style-type: none"> <li>1. The acquisition of personal information does not create a material risk of identity theft or fraud to the subject of the personal information.</li> <li>2. The personal information was acquired in good faith by an employee or agent of the entity, if the personal information is used for a lawful purpose of the entity.</li> </ol>		<p>The entity shall make reasonable efforts to notify each resident of this state who is the subject of the personal information. The notice shall indicate that the entity knows of the unauthorized acquisition of personal information pertaining to the resident of this state who is the subject of the personal information.</p> <p>Subject to [requests by law enforcement] an entity shall provide the notice within a reasonable time, not to exceed 45 days after the entity learns of the acquisition of personal information. A determination as to reasonableness under this paragraph shall include consideration of the number of notices that an entity must provide and the methods of communication available to the entity. An entity shall provide the notice by mail or by a method the entity has previously employed to communicate with the subject of the personal information. If an entity cannot with reasonable diligence determine the mailing address of the subject of the personal information, and if the entity has not previously communicated with the subject of the personal information, the entity shall provide notice by a method reasonably calculated to provide actual notice to the subject of the personal information. If as the result of a single incident, an entity is required under to notify 1,000 or more individuals that personal information pertaining to the individuals has been acquired, the entity shall without unreasonable delay notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in <u>15 USC 1681a(p)</u>, of the timing, distribution, and content of the notices sent to the individuals.</p>

**STATE LAW: SECURITY BREACH NOTIFICATION**

<b>State</b>	<b>“Personal Information”</b>	<b>“Breach”</b>	<b>Exceptions</b>	<b>Destruction of Records and Security Policies</b>	<b>Disclosure of Breaches</b>
<p><b>WY</b> WY-ST 40-12- 501</p>	<p>“Personal identifying information” means the first name or first initial and last name of a person in combination with (1) or more of the following data elements when either the name or the data elements are not redacted: (a) SS number; (b) Driver’s license number or ID number; (c) Account number, credit card number or debit card number in combination with any security code, access code or password that would allow access to a financial account of the person; (d) Tribal identification card; (e) Federal or state government issued ID card.</p>	<p>“Breach of the security of the data system” means unauthorized acquisition of the computerized data that materially compromises the security, confidentiality or integrity of personal identifying information maintained by a person or business and causes or is reasonably believe to cause loss or injury to a resident of the state.</p>	<p>Good faith acquisition of personal identifying information by an employee or agent of a person or business for the purposes of the person or business is not a breach of the security of the data system, provided that the personal identifying information is not used or subject to further unauthorized disclosure.</p>		<p>An 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 shall, when it becomes aware of a breach of the security of the system, conduct in good faith a reasonably and prompt investigation to determine the likelihood that personal identifying information has been or will be misused. If the investigation determines that the misuse of personal identifying information about a resident has occurred or is likely to occur, the individual of the commercial entity shall give notice as soon as possible to the affected Wyoming resident. 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 to consumers may be provided by written notice, electronic mail notice, or substitute notice if: (a) The person demonstrates that the cost of providing notice would exceed \$10,000 for Wyoming based persons or businesses, and \$250,000 for all other business operating but not based in Wyoming; (b) The affected class of subject persons to be notified exceeds 10,000 for Wyoming based persons or business and 500,000 for all other businesses operating but not based in Wyoming; or (c) The person does not have sufficient contact information.</p>