

STATE-BY-STATE BREACH NOTIFICATION LAW AND REQUIREMENTS

STATE	APPLICABLE LAW	DATE ENACTED	SAFE HARBOR FOR ENCRYPTED DATA	WHO IS SUPPOSED TO BE NOTIFIED	WHEN ARE THEY SUPPOSED TO BE NOTIFIED	HOW ARE THEY SUPPOSED TO BE NOTIFIED	SPECIAL RESTRICTIONS
Alaska	2008 H.B. 65 http://www.legis.state.ak.us/PDF/25/Bills/HB0065Z.PDF	7/1/2009	Undefined	If a covered person owns or licenses personal information in any form that includes personal information on a state resident, and a breach of the security of the information system that contains personal information occurs, the covered person shall, after discovering or being notified of the breach, disclose the breach to each state resident whose personal information was subject to the breach.	An information collector shall make the disclosure required by (a) of this section in the most expeditious time possible and without unreasonable delay, except, as provided in AS 45.48.202 and as necessary to determine the scope of the breach and restore the reasonable integrity of the information system. Notwithstanding (a) of this section, disclosure is not required if, after an appropriate investigation and after written notification to the attorney general of this state, the covered person determines that there is not a reasonable likelihood that harm to the consumers whose personal information has been acquired has resulted or will result from the breach. The determination shall be documented in writing, and the documentation shall be maintained for five years. the notification required by this subsection may not be considered a public record open to inspection by the public.	1) By a written document sent to the most recent address the information collector has for the state resident; 2) By electronic means if the information collector's primary method of communication with the state resident is by electronic means or if making the disclosure by the electronic means is consistent with the provisions regarding electronic records and signature required for notices legally required to be in writing under 15 U.S.C. 7001 et seq. (Electronic Signatures in Global and National Commerce Act); 3) if the information collector demonstrates that the cost of providing notice would exceed \$150,000, that the affected class of state residents to be notified exceeds 300,000, or that the information collector does not have sufficient contact information to provide notice, by: i) Electronic mail if the information collector has an electronic mail address for the state resident; ii) Conspicuously posting the disclosure on the Internet website of the information collector if the information collector maintains an Internet website; iii) Providing a notice to major statewide media	Yes
Arizona	Ariz. Rev. Stat. § 44-7501 SB 1388	1/1/2007	Yes	Anyone who conducts business in this state and that owns or licenses unencrypted computerized data that becomes aware of an incident of unauthorized acquisition and access to unencrypted or unredacted computerized data shall notify the individuals affected.	After determination of a breach in the most expedient manner possible and without unreasonable delay subjected to the needs of law enforcement	1) Electronic notice if the person's primary method of communication with the individual is by electronic means 2) Conspicuous posting of the notice on the web site of the person if the person maintains one. 3) Notification to major statewide media.	
Arkansas	Arkansas SB 1167	8/12/2005	Yes	Any resident of Arkansas	Most expedient time and manner possible and without unreasonable delay consistent with the legitimate needs of law enforcement	1) Written or 2) Electronic Mail or 3) Conspicuous posting of the notice on the website of the person or business, if they maintain one 4) Statewide Media	

STATE-BY-STATE BREACH NOTIFICATION LAW AND REQUIREMENTS

<p>California</p>	<p>Cal. Civ. Code §§ 56.06, 1785.11.2, 1798.29, 1798.82 SB 1386</p>	<p>7/1/2003</p>	<p>Yes</p>	<p>Any person or business that conducts 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.</p> <p>Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.</p>	<p>The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.</p>	<p>1) Written notice, 2) Telephonic Notice, 3) Electronic Notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code. 4) Substitute Notice a) E-mail Notice when the person or business has an e-mail address for the subject persons b) Conspicuous Posting of the notice on the Web site page of the person or business, if the person or business maintains one c) Notification to major statewide media d) Notwithstanding subdivision (g), a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part, shall be deemed to be in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.</p>	<p>Yes</p>
--------------------------	---	-----------------	------------	--	--	--	------------

STATE-BY-STATE BREACH NOTIFICATION LAW AND REQUIREMENTS

Colorado	Session Laws of Colorado, 2006, 65 General Assembly, Chapter 145 SB 06-1119	9/1/2006	Yes	Colorado Resident	Most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement §d All consumer reporting agencies	1) Written Notice, 2) Telephonic Notice, 3) Electronic Notice 4) Email Notice 5) Conspicuous Posting on the web site page of the individual or commercial entity 6) Major Statewide Media	
Connecticut	Conn. Gen Stat. 36a-701(b) SB 650	1/1/2006	Yes	Any Connecticut resident	Any person that maintains computerized data that includes personal information that the person does not own shall notify the owner of licensee of the information of any breach of the security of the data immediately following its discovery. Notification shall be delayed for a reasonable period of time if a law enforcement agency determines that the notification will impede a criminal investigation.	1) Written notice, 2) Telephonic Notice, 3) Electronic Notice 4) Substitute Notice a) Email Notice b) Conspicuous Posting on the web site page of the individual or commercial entity c) Major Statewide Media (newspapers, radio, & television)	
Delaware	Del. Code tit. 6, § 12B-101 et seq. HB 116	6/28/2005	Yes	An individual or a commercial entity that conducts business in Delaware and that owns or licenses computerized data that includes personal information about a resident of Delaware 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.	The individual or the commercial entity shall give notice as soon as possible to the affected Delaware resident. Notice must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement	1) Written notice, 2) Telephonic Notice, 3) Electronic Notice 4) Substitute Notice a) Email Notice b) Conspicuous Posting on the web site page of the individual or commercial entity c) Major Statewide Media	
Florida	Fla. Stat. § 817.5681 HB 481	7/1/2005	Yes	any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.	The notification shall be made without unreasonable delay, consistent with the legitimate needs of law enforcement, or subject to any measures necessary to determine the presence, nature, and scope of the breach and restore the reasonable integrity of the system. Notification must be made no later than 45 days following the determination of the breach unless otherwise provided in this section. Any person who maintains computerized data that includes personal information on behalf of another business entity shall disclose to the business entity for which the information is maintained any breach of the security of the system as soon as practicable, but no later than 10 days following the determination, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.	1) Written notice, 2) Electronic Notice 3) Substitute Notice a) Email Notice b) Conspicuous Posting on the web site page of the individual or commercial entity c) Major Statewide Media (newspapers, radio, & television)	Yes

STATE-BY-STATE BREACH NOTIFICATION LAW AND REQUIREMENTS

Georgia	Ga. Code §§ 10-1-910, -911 SB 230	5/5/2005	Yes	<p>Any investigative consumer reporting agency that owns or licenses files or 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 or file was, or is reasonably believed to have been, acquired by an unauthorized person.</p> <p>Any investigative consumer reporting agency that maintains computerized data that includes personal information of individuals that the investigative consumer reporting agency does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.</p>	The notice shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (c) of this Code section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.	<p>1) Written notice, 2) Telephonic Notice, 3) Electronic Notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of title 15 of the United States Code 4) Substitute Notice a) Email Notice, if the investigative consumer reporting agency has an e-mail address for the individuals to be notified; b) Conspicuous posting of the notice on the investigative consumer reporting agency's website page, if the agency maintains one; and c) Notification to major state-wide media Notwithstanding any provision of this paragraph to the contrary, an investigative consumer reporting agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this article shall be deemed to be in compliance with the notification requirements of this article shall be deemed to be in compliance with the notification requirements of this article if it notifies the individuals who are the subjects of the notice in accordance with its policies in the event of a breach of the security of the system.</p>	Yes
Hawaii	Haw. Rev. Stat. § 487N-2 SB 2290	1/1/2007	Yes	Any business located in Hawaii or any business that conducts business in Hawaii that maintains or possesses records or data containing personal information of residents of Hawaii that the business does not own or license, or any government agency that maintains or possesses records or data containing personal information of residents of Hawaii	Shall notify the owner or licensee of the information of any security breach immediately following discovery of the breach, consistent with the legitimate needs of law enforcement as provided in subsection	<p>1) Written notice, 2) Electronic Notice 3) Telephonic Notice, 3) Substitute Notice a) Email Notice b) Conspicuous Posting on the web site page of the individual or commercial entity c) Major Statewide Media</p>	Yes
Idaho	Idaho Code §§ 28-51-104 to 28-51-107 SB 1374	7/1/2006	Yes	An agency, individual or a commercial entity that conducts business in Idaho and that owns or licenses computerized data that includes personal information about a resident of Idaho.	Notice must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach, to identify the individuals affected, and to restore the reasonable integrity of the computerized data system.	<p>1) Written notice to the most recent address the agency, individual or commercial entity has in its records; 2) Telephonic notice; 3) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. section 7001; 3) Substitute Notice a) E-mail notice, if the agency, individual or the commercial entity has e-mail addresses for the affected Idaho residents; b) Conspicuous posting of the notice on the website page of the agency, individual or the commercial entity if the agency, individual or the</p>	
Illinois	815 ILCS 530/1 et seq. HB 1633	1/1/2006	Yes	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>1) Written notice, 2) Electronic Notice 3) Substitute Notice a) Email Notice b) Conspicuous Posting on the web site page of the individual or commercial entity c) Major Statewide Media</p>	Yes

STATE-BY-STATE BREACH NOTIFICATION LAW AND REQUIREMENTS

<p>Indiana</p>	<p>Ind. Code §§ 24-4.9 et seq., 4-1-11 et seq. SB 503 HB 1101</p>	<p>7/1/2006</p>	<p>Yes</p>	<p>A business entity that owns or licenses a computerized data system that includes personal information shall disclose any breach of the security of the system after the discovery of the breach to any resident of the state whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person.</p>	<p>Subject to section 6 of this chapter, a disclosure made under subsection (a) must be made as soon as possible after the breach is discovered consistent with any measures taken by the business entity that are necessary to: (1) determine the scope of the breach; and (2) restore the reasonable integrity of the data system</p>	<p>1) Written notice, 2) Electronic notice if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. 7001 et seq. 3) Substitute Notice a) Electronic mail notice, if the business entity has an electronic mail address for a person that must be notified; b) If the business entity maintains an Internet web site, conspicuous posting of the notice on the business entity's web site; c) Notification to major statewide news media</p>	
<p>Iowa</p>	<p>Iowa Code § 715C.1 (2008, S.F. 2308)</p>	<p>7/1/2008</p>	<p>Yes</p>	<p>Any person who 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.</p>	<p>The consumer notification shall be made in the most expeditious manner possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to sufficiently determine contact information for the affected consumers, determine the scope of the breach, and restore the reasonable integrity, security, and confidentiality of the data.</p>	<p>1) Written notice, 2) Electronic Notice 3) Substitute Notice a) Email Notice b) Conspicuous Posting on the web site page of the individual or commercial entity c) Major Statewide Media (newspapers, radio, & television)</p>	<p>Yes</p>
<p>Kansas</p>	<p>Kan. Stat. 50-7a01, 50-7a02 SB 196</p>	<p>7/1/2006</p>	<p>Yes</p>	<p>A person that conducts business in this state, or a government, governmental subdivision or agency that owns or licenses computerized data that includes personal information shall, when it becomes aware of any breach of the security of the system, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused. If the investigation determines that the misuse of information has occurred or is reasonably likely to occur, the person or government, governmental subdivision or agency shall give notice as soon as possible to the affected Kansas resident.</p>	<p>Notice must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.</p>	<p>1) Written notice 2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. 7001; 3) Substitute notice; i) E-mail notice if the individual or the commercial entity has e-mail addresses for the affected class of consumers ii) Conspicuous posting of the notice on the web site page of the individual or the commercial entity if the individual or the commercial entity maintains a web site; iii) Notification to major statewide media</p>	<p>Yes</p>
<p>Louisiana</p>	<p>La. Rev. Stat. § 51:3071 et seq. SB 205</p>	<p>1/1/2006</p>	<p>N/A</p>	<p>Any person that conducts business in the state or that owns or licenses computerized data that includes personal information, or any agency that owns or licenses computerized data that includes personal information Any agency or person that maintains computerized data that includes personal information that the agency or person does not own shall notify the owner or licensee of the information if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person through a breach of security of the system containing such data, following discovery by the agency or person of a breach of security of the system.</p>	<p>following discovery of a breach in the security of the system containing such data, notify any resident of the state whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The notification required pursuant to Subsections A and B of this Section shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in Subsection D of this Section, or any measures necessary to determine the scope of the breach, prevent further disclosures, and restore the reasonable integrity of the data system.</p>	<p>1) Written notice, 2) Electronic Notice 3) Substitute Notice a) Email Notice b) Conspicuous Posting on the web site page of the individual or commercial entity c) Major Statewide Media</p>	

STATE-BY-STATE BREACH NOTIFICATION LAW AND REQUIREMENTS

<p>Maine</p>	<p>Me. Rev. Stat. tit. 10 §§. 1347 et seq. LD 1671</p>	<p>1/31/2006</p>	<p>Yes</p>	<p>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.</p> <p>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.</p>	<p>The notices must be made as expeditiously as possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or with measures necessary to determine the scope of the security breach and restore the reasonable integrity, security and confidentiality of the data in the system.</p> <p>A 3rd-party entity that maintains, on behalf of a person, computerized data that includes personal information that the 3rd-party entity does not own shall notify the person maintaining personal information of a breach of the security of the system immediately following discovery if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.</p>	<p>1) Written notice 2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 United States Code, Section 7001; 3) Substitute notice; i) E-mail notice if the person has e-mail addresses for the individuals to be notified; ii) Conspicuous posting of the notice on the person's publicly accessible website, if the person maintains one; iii) Notification to major statewide media</p>	<p>Yes; When notice of a breach of the security of the system is required under subsection 1, the person shall notify the appropriate state regulators within the Department of Professional and Financial Regulation, or if the person is not regulated by the department, the Attorney General.</p>
<p>Maryland</p>	<p>Md. Code. Com. Law § 14-3501 et seq. HB 208 SB 194</p>	<p>1/1/2008</p>	<p>Undefined</p>	<p>A business that owns or licenses computerized data that includes personal information of an individual residing in the State, when it discovers or is notified of a breach of the security of a system, shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information of the individual has been or will be misused as a result of the breach.</p> <p>A business that maintains computerized data that includes personal information that the business does not own or license shall notify the owner or licensee of the personal information of a breach of the security of a system if it is likely that the breach has resulted or will result in the misuse of personal information of an individual residing in the State.</p>	<p>Except as provided in subsection (d) of this section, the notification required under paragraph (1) of this subsection shall be given as soon as reasonably practicable after the business discovers or is notified of the breach of the security of a system.</p>	<p>1) Written notice, 2) Electronic Notice 3) Telephonic Notice, 4) Substitute Notice a) Email Notice b) Conspicuous Posting on the web site page of the individual or commercial entity c) Major Statewide Media</p>	

STATE-BY-STATE BREACH NOTIFICATION LAW AND REQUIREMENTS

<p>Massachusetts</p>	<p>Mass. Gen. Laws § 93H-1 et seq. SB 2058 HB 4144</p>	<p>2/3/2008</p>	<p>Undefined</p>	<p>A person or agency that maintains or stores, but does not own or license data that includes personal information about a resident of the commonwealth, shall provide notice, as soon as practicable and without unreasonable delay, when such person or agency (1) knows or has reason to know of a breach of security or (2) when the person or agency knows or has reason to know that the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose, to the owner or licensor in accordance with this chapter.</p>	<p>A person or agency that owns or licenses data that includes personal information about a resident of the commonwealth, shall provide notice, as soon as practicable and without unreasonable delay, when such person or agency (1) knows or has reason to know of a breach of security or (2) when the person or agency knows or has reason to know that the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose, to the attorney general, the director of consumer affairs and business regulation and to such resident, in accordance with this chapter. The notice to be provided to the attorney general and said director, and consumer reporting agencies or state agencies if any, shall include, but not be limited to, the nature of the breach of security or unauthorized acquisition or use, the number of residents of the commonwealth affected by such incident at the time of notification, and any steps the person or agency has taken or plans to take relating to the incident.</p>	<p>1) Written notice, 2) Electronic Notice 3) Substitute Notice a) Email Notice b) Clear and conspicuous posting of the notice on the home page of the person or agency if the person or agency maintains a website c) publication in or broadcast through media or medium that provides notice throughout the commonwealth</p>	<p>Yes; The attorney general may bring an action pursuant to section 4 of chapter 93A against a person or otherwise to remedy violations of this chapter and for other relief that may be appropriate.</p>
<p>Michigan</p>	<p>Mich. Comp. Laws § 445.72 SB 308 HB 4568</p>	<p>6/29/2007</p>	<p>Yes</p>	<p>Unless the person or agency determines that the security breach has not or is not likely to cause substantial loss or injury to, or result in identity theft with respect to, 1 or more residents of this state, a person or agency that owns or licenses data that are included in a database that discovers a security breach, or receives notice of a security breach under subsection (2), shall provide a notice of the security breach to each resident of this state who meets 1 or more of the following: (a) That resident's unencrypted and unredacted personal information was accessed and acquired by an unauthorized person. (b) That resident's personal information was accessed and acquired in encrypted form by a</p>	<p>A person or agency shall provide any notice required without unreasonable delay. A person or agency may delay providing notice if either of the following is met: (a) A delay is necessary in order for the person or agency to take any measures necessary to determine the scope of the security breach and restore the reasonable integrity of the database. (b) A law enforcement agency determines and advises the agency or person that providing a notice will impede a criminal or civil investigation or jeopardize homeland or national security.</p>	<p>1) Written notice, 2) Electronic Notice 3) Telephonic Notice, 4) Substitute Notice a) Email Notice b) Conspicuous Posting on the web site page of the individual or commercial entity c) Major Statewide Media. (a notification under this shall include a telephone number or a website address that a person may use to obtain additional assistance and information)</p>	<p>Yes</p>
<p>Minnesota</p>	<p>https://www.revisor.leg.state.mn.us/bin/bldbill.php?bill=H.2121.3&session=ls84 HF 2121</p>	<p>1/1/2006</p>	<p>Yes</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. Any person or business that maintains data that includes person information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.</p>	<p>The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or with any measures necessary to determine the scope of the breach, identify the individuals affected, and restore the reasonable integrity of the data system.</p>	<p>1) Written notice, 2) Electronic Notice 3) Substitute Notice a) Email Notice b) Clear and conspicuous posting of the notice on the Web site page of the person or business, if the person or business maintains one c) notification to major statewide media</p>	

STATE-BY-STATE BREACH NOTIFICATION LAW AND REQUIREMENTS

<p>Montana</p>	<p>Mont. Code S. 30-14-1701 et seq. HB 732</p>	<p>3/1/2006</p>	<p>Yes</p>	<p>Any resident of Montana</p>	<p>The disclosure must be made without unreasonable delay, consistent with the legitimate needs of law enforcement, or consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.</p>	<p>1) Written notice, 2) Electronic Notice 3) Telephonic Notice, 4) Substitute Notice a) Email Notice b) Conspicuous Posting on the web site page of the individual or commercial entity c) Major Statewide Media, (a notification under this shall include a telephone number or a website address that a person may use to obtain additional assistance and information)</p>	
<p>Nebraska</p>	<p>Neb. Rev. Stat. §§ 87-801, -802, -803, -804, -805, -806, -807 LB 876</p>	<p>4/6/2006</p>	<p>Undefined</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.</p> <p>An individual or a commercial entity that maintains computerized data that includes personal information that the individual or commercial entity does not own or license shall give notice to and cooperate with the owner or licensee of the information of any breach of the security of the system when it becomes aware of a breach if use of personal information about a Nebraska resident for an unauthorized purpose occurred or is reasonably likely to occur. Cooperation includes, but is not limited to, sharing with the owner or licensee information relevant to the breach, not including information proprietary to the individual or commercial entity.</p>	<p>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, 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>(a) Written notice; (b) Telephonic notice; (c) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. 7001, as such section existed on January 1, 2006; (d) Substitute notice, (i) Electronic mail notice if the individual or commercial entity has electronic mail addresses for the members of the affected class of Nebraska residents; (ii) Conspicuous posting of the notice on the web site of the individual or commercial entity if the individual or commercial entity maintains a web site; and (iii) Notice to major statewide media outlets; or</p>	<p>Yes; Substitute notice requirements</p>
<p>Nevada</p>	<p>Nev. Rev. Stat. 603A.010 et seq. SB 347 HF 2121</p>	<p>1/1/2006</p>	<p>Yes</p>	<p>Resident of this State</p>	<p>The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement Any data collector that maintains computerized data which includes personal information that the data collector does not own shall notify the owner or licensee of the information of any breach of the security of the system data immediately following discovery if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.</p>	<p>1) Written notice, 2) Electronic Notice 3) Telephonic Notice, 4) Substitute Notice a) Email Notice b) Conspicuous Posting on the web site page of the individual or commercial entity c) Major Statewide Media</p>	

STATE-BY-STATE BREACH NOTIFICATION LAW AND REQUIREMENTS

New Hampshire	N.H. Rev. Stat. §§ 359-C:19, -C:20, -C:21 HB 1660	1/1/2007	Undefined	<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>Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify and cooperate with the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was acquired by an unauthorized person. Cooperation includes sharing with the owner or licensee information relevant to the breach; except that such cooperation shall not be deemed to require the disclosure of confidential or business information or trade secrets.</p>	<p>Any person engaged in trade or commerce that is subject to RSA 358-A:3, I shall also notify the regulator which has primary regulatory authority over such trade or commerce. All other persons shall notify the New Hampshire attorney general's office. The notice shall include the anticipated date of the notice to the individuals and the approximate number of individuals in this state who will be notified. Nothing in this section shall be construed to require the person to provide to any regulator or the New Hampshire attorney general's office the names of the individuals entitled to receive the notice or any personal information relating to them. The disclosure shall be made to affected individuals as quickly as possible, after the determination required under this section.</p>	<p>(a) Written notice; (b) Electronic notice, if the agency or business' primary means of communication with affected individual is by electronic means; (c) Telephonic notice, provided that a log of each such notification is kept by the person or business who notifies affected persons; (d) Substitute notice, (i) E-mail notice when the person has an e-mail address for the affected individuals; (ii) Conspicuous posting of the notice on the person's business website, if the person maintains one; (iii) Notification to major statewide media (e) Notice pursuant to the person's internal notification procedures maintained as part of an information security policy for the treatment of personal information</p>	Yes
New Jersey	N.J. Stat. 56:8-163 A-4001	1/1/2006	Yes	Any resident of this State	<p>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. Any business or public entity that compiles or maintains computerized records that include personal information on behalf of another business or public entity shall notify that business or public entity, who shall notify its New Jersey customer, of any breach of security of the computerized records immediately following discovery, if the personal information was, or is reasonably believed to have been, accessed by an unauthorized person.</p>	<p>1) Written notice, 2) Electronic Notice 3) Telephonic Notice, 4) Substitute Notice a) Email Notice b) Conspicuous Posting on the web site page of the business or public entity, if the business or public entity maintains one; and c) Major Statewide Media</p>	
New York	N.Y. Gen. Bus. Law § 899-aa http://www.cscic.state.ny.us/security/securitybreach/ A-4254	12/7/2005	Yes	Any New York state resident	<p>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. Any state entity that maintains computerized data that includes private information which such agency does not own shall notify the owner or licensee of the information of any reach of the security of the system immediately following discovery, if the private information was, or is reasonably believed to have been, acquired by a person without valid authorization.</p>	<p>1) Written notice, 2) Electronic Notice 3) Telephone notification provided that a log of each such notification is kept by the state entity who notifies affected persons 4) Substitute Notice a) Email notice when such state entity has an e-mail address for the subject persons; b) Conspicuous posting of the notice on such state entity's web site page, if such agency maintains one; c) notification to major statewide media</p>	<p>Yes; The state entity shall consult with the state office of cyber security and critical infrastructure coordination to determine the scope of the breach and restoration measures. Other restrictions apply.</p>

STATE-BY-STATE BREACH NOTIFICATION LAW AND REQUIREMENTS

<p>North Carolina</p>	<p>N.C. Gen. Stat § 75-65 SB 1048</p>	<p>12/1/2005</p>	<p>Yes</p>	<p>Any North Carolina resident</p> <p>Any business that maintains or possesses records or data containing personal information of residents of North Carolina that the business does not own or license, or any business that conducts business in North Carolina that maintains or possesses records or data containing personal information that the business does not own or license shall notify the owner or licensee of the information of any security breach immediately following discovery of the breach, consistent with the legitimate needs of law enforcement.</p>	<p>The disclosure notification shall be made without unreasonable delay, consistent with the legitimate needs of law enforcement, and consistent with any measures necessary to determine sufficient contact information, determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.</p>	<p>1) Written notice, 2) Electronic Notice 3) Telephonic notice provided that contact is made directly with the affected persons. 4) Substitute Notice a) Email notice when such the business has an electronic mail address for the subject persons; b) Conspicuous posting of the notice on the Web page of the business, if one is maintained; c) Notification to major statewide media</p>	<p>Yes;</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</p>
<p>North Dakota</p>	<p>N.D. Cent. Code § 51-30-01 et seq. FRBS-0500 SB 2251</p>	<p>6/1/2005</p>	<p>Yes</p>	<p>Any resident of North Dakota</p> <p>Any person that conducts business in this state, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of the state whose unencrypted personal information was or is reasonably believed to have been, acquired by an unauthorized person.</p> <p>Any person that maintains computerized data that includes personal information that the person does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following the discovery, if the personal information was, or is reasonably believed to have been acquired by an unauthorized person.</p>	<p>The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or any measures necessary to determine the scope of the breach and to restore the integrity of the data system.</p>	<p>1) Written notice, 2) Electronic Notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in section 7001 of title 15 of the United States Code; 3) Substitute Notice a) Email notice when the person has an e-mail address for the subject persons; b) Conspicuous posting of the notice on the person's web site page; if the person maintains one; c) notification to major statewide media</p>	<p>Yes</p>

STATE-BY-STATE BREACH NOTIFICATION LAW AND REQUIREMENTS

<p>Ohio</p>	<p>Ohio Rev. Code §§ 1347.12, 1349.19, 1349.191, 1349.192 HB 104</p>	<p>2/17/2006</p>	<p>Undefined</p>	<p>Any state agency or agency of a political subdivision 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 state agency or agency of a political subdivision shall make the disclosure described in division (B)(1) of this section in the most expedient time possible but not later than forty-five days following its discovery or notification of the breach in the security of the system, subject to the legitimate needs of law enforcement activities described in division (D) of this section and consistent with any measures necessary to determine the scope of the breach, including which residents' personal information was accessed and acquired, and to restore the reasonable integrity of the data system.</p> <p>Any state agency or agency of a political subdivision that, on behalf of or at the direction of another state agency or agency of a political subdivision, is the custodian of or stores computerized data that includes personal information shall notify that other state agency or agency of a political subdivision of any breach of the security of the system in an expeditious manner, if the personal information was, or reasonably is believed to have been, accessed and acquired by an unauthorized person and 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 a resident of this state.</p>	<p>1) Written notice, 2) Electronic Notice, if the state agency's or agency of a political subdivision's primary method of communication with the resident to whom the disclosure must be made is by electronic means; 3) Telephonic notice; 4) Substitute Notice a) Electronic mail notice if the state agency or agency of a political subdivision has an electronic mail address for the resident to whom the disclosure must be made; b) Conspicuous posting of the disclosure or notice on the state agency's or agency of a political subdivision's web site, if the agency maintains one; c) Notification to major media outlets to the extent that the cumulative total of the readership, viewing audience, or listening audience of all of the outlets so notified equals or exceeds seventy-five per cent of the population of this state</p>	<p>Yes;</p>
<p>Oklahoma</p>	<p>Okla. Stat. § 74-3113.1 and 2008 H.B. 2245 HB 2357</p>	<p>6/8/2006</p>	<p>Undefined</p>	<p>Any state agency, board, commission or other unit or subdivision of state government that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of Oklahoma whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.</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, as provided in subsection C of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.</p> <p>Any state agency, board, commission or other unit or subdivision of state government that maintains computerized data that includes personal information that the state agency, board, commission or other unit or subdivision of state government does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.</p>	<p>1) Written notice, 2) Electronic Notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in section 7001 of title 15 of the United States Code; 3) Substitute Notice a) E-mail notice when the agency has an e-mail address for the subject persons; b) Conspicuous posting of the notice on the agency's web site page; if the agency maintains one,; c) notification to major statewide media</p>	<p></p>

STATE-BY-STATE BREACH NOTIFICATION LAW AND REQUIREMENTS

Oregon	2007 S.B. 583, Chapter 759	10/1/2007	Undefined	<p>Any person that owns, maintains or otherwise possesses data that includes a consumer's personal information that is used in the course of the person's business, vocation, occupation or volunteer activities and was subject to a breach of security shall give notice of the breach of security following discovery of such breach of security, or receipt of notification, to any consumer whose personal information was included in the information that was breached.</p> <p>Any person that 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.</p>	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 reasonable integrity, security and confidentiality of the data.	<p>1) Written notice, 2) Electronic Notice if the person's customary method of communication with the consumer is by electronic means or is consistent with the provisions regarding electronic records and signatures set forth in the Electronic Signatures in Global and National Commerce Act as that Act existed on the effective date of this 2007 Act 3) Telephonic notice provided that contact is made directly with the affected persons. 4) Substitute Notice a) Conspicuous posting of the notice on or a link to the notice on the Internet home page of the person if the person maintains one; b) Notification to major statewide television and newspaper media</p>	<p>Yes</p> <p>Consumer vs resident Dollar amount of breach</p>
Pennsylvania	http://www2.legis.state.pa.us/WU01/LI/BI/BT/2005/0/SB0712P1410.pdf SBG 712	6/20/2006	Yes	<p>An entity that maintains, stores or manages computerized data that includes personal information shall provide notice of the 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.</p> <p>For the purpose of this section, a resident of this Commonwealth may be determined to be an individual whose principal mailing address, as reflected in the computerized data which is maintained, stored or managed by the entity, is in this Commonwealth.</p> <p>A vendor that maintains, stores or manages computerized data on behalf of another entity shall provide notice of any breach of the security system following discovery by the vendor to the entity on whose behalf the vendor maintains, stores or manages the data. The entity shall be responsible for making the determinations and discharging any remaining duties under this act.</p>	An entity that maintains, stores or manages computerized data that includes personal information shall provide notice of the 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.	<p>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 a) Email notice when the entity has an e-mail address for the subject persons; b) Conspicuous posting of the notice on the entity's Internet website if the entity maintains one; c) Notification to major statewide media</p>	<p>Yes;</p>

STATE-BY-STATE BREACH NOTIFICATION LAW AND REQUIREMENTS

<p>Rhode Island</p>	<p>R.I. Gen. Laws § 11-49.2-1 et seq. HB 6191</p>	<p>3/1/2006</p>	<p>Yes</p>	<p>Any state agency or person that owns, maintains or licenses computerized data that includes personal information, shall disclose any breach of the security of the system which poses a significant risk of identity theft following discovery or notification of the breach in the security of the data to any resident of Rhode Island whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person or a person without authority, to acquire said information.</p> <p>Any state agency or person that maintains computerized unencrypted data that includes personal information that the state agency or person does not own shall notify the owner or licensee of the information of any breach of the security of the data which poses a significant risk of identity theft immediately, following discovery, if the 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 any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.</p> <p>The notification must be prompt and reasonable following the determination of the breach unless otherwise provided in this section. Any state agency or person required to make notification under this section and who fails to do so promptly following the determination of a breach or receipt of notice from law enforcement as provided for in subsection (c) is liable for a fine as set forth in § 11-49.2-6.</p>	<p>1) Written notice, 2) Electronic Notice if the notice provided is consistent with the provisions regarding electronic records and signatures set for the in Section 7001 of Title 15 of the United States Code; 3) Substitute Notice a) Conspicuous posting of the notice on the state agency's or person's website page, if the state agency or person maintains one; b) Notification to major statewide media</p>	<p>Yes</p>
<p>South Carolina</p>	<p>2008 S.B. 453, Act 190</p>	<p>12/31/2008</p>	<p>Undefined</p>	<p>An agency of this State owning or licensing computerized data or other data that includes personal identifying information shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of this State whose unencrypted and unredacted personal identifying information was, or is reasonably believed to have been, acquired by an unauthorized person when the illegal use of the information has occurred or is reasonably likely to occur or use of the information creates a material risk of harm to the resident.</p> <p>An agency maintaining computerized data or other data that includes personal identifying information that the agency does not own shall notify the owner or licensee of the information of a breach of the security of the data immediately following discovery, if the personal identifying information was, or is reasonably believed to have been, acquired by an unauthorized person.</p>	<p>The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or with measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.</p>	<p>1) Written notice 2) Electronic notice, if the person's primary method of communication with the individual is by electronic means or is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 USC and Chapter 6, Title 26 of the 1976 Code; 3) Telephonic notice, 4) Substitute Notice a) Email notice when the agency has an e-mail address for the subject persons; b) Conspicuous posting of the notice on the agency's web site page, if the agency maintains one; c) Notification to major statewide media</p>	<p></p>

STATE-BY-STATE BREACH NOTIFICATION LAW AND REQUIREMENTS

Tennessee	Tenn. Code § 47-18-2107 HB 2170	7/1/2005	Yes	<p>Any information holder shall disclose any breach of the security of the system, following discovery or notification of the breach in the security of the data, to any resident of Tennessee whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.</p> <p>Any information holder that maintains computerized data that includes personal information that the information holder does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.</p>	The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.	<p>1) Written notice, 2) Electronic Notice if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C., section 7001; 3) Substitute Notice a) E-mail notice, when the information holder has an e-mail address for the subject persons; b) Conspicuous posting of the notice on the information holder's internet website page, if the information holder maintains such website page; c) Notification to major statewide media</p>	
Texas	http://www.statutes.legis.state.tx.us/DocViewer.aspx?K2DocKey=odbc%3a%2f%2fSOTW%2fASUPUBLIC.dbo.vwSOTW%2fBC%2fS%2fBC.521%40SOTW&QueryText=breach%3cOR%3enotification&HighlightType=1. SB 122	9/1/2005	Yes	<p>A person who conducts business in this state and owns or licenses computerized data that includes sensitive personal information shall disclose any breach of system security, after discovering or receiving notification of the breach, to any resident of this state whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person.</p> <p>Any person who maintains computerized data that includes sensitive personal information not owned by the person shall notify the owner or license holder of the information of any breach of system security immediately after discovering the breach, if the sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person.</p>	The disclosure shall be made as quickly as possible, or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system.	<p>1) Written notice 2) Electronic notice, if the notice is provided in accordance with 15 U.S.C. Section 7001; 3) Substitute Notice a) Electronic mail, if the person has electronic mail addresses for the affected persons; b) Conspicuous posting of the notice on the person's website; c) Notice published in or broadcast on major statewide media</p>	
Utah	Utah Code §§ 13-44-101, -102, -201, -202, -310 SB 0069	1/1/2007	No	<p>A person who owns or licenses computerized data that includes personal information concerning a Utah resident</p> <p>A person who maintains computerized data that includes personal information that the person does not own or license shall notify and cooperate with the owner or licensee of the information of any breach of system security immediately following the person's discovery of the breach if misuse of the personal information occurs or is reasonably likely to occur.</p>	<p>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>A person required to provide notification under Subsection (1) shall provide the notification in the most expedient time possible without unreasonable delay: (a) considering legitimate investigative needs of law enforcement;; (b) after determining the scope of the breach of system security; and (c) after restoring the reasonable integrity of the system.</p>	<p>1) In writing by first-class mail to the most recent address the person has for the resident; 2) 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; 3) by telephone, including through the use of automatic dialing technology not prohibited by other law; 4) by publishing notice of the breach of system security 5) in a newspaper of general circulation; and 45-1-101.</p>	Yes

STATE-BY-STATE BREACH NOTIFICATION LAW AND REQUIREMENTS

<p>Vermont</p>	<p>Vt. Stat. tit. 9 § 2430 et seq. SB 284</p>	<p>1/1/2007</p>	<p>Yes</p>	<p>Any data collector that owns or licenses computerized personal information that includes personal information concerning a consumer shall notify the consumer that there has been a security breach following discovery or notification to the data collector of the breach.</p> <p>Any data collector that maintains or possesses computerized data containing personal information of a consumer that the business does not own or license or any data collector that conducts business in Vermont that maintains or possesses records or data containing personal information that the data collector does not own or license shall notify the owner or licensee of the information of any security breach immediately following discovery of the breach, consistent with the legitimate needs of law enforcement</p>	<p>Notice of the breach shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of the law enforcement agency, 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>1) Written notice mailed to the consumer's residence; 2) Electronic notice, for those consumers for whom the data collector has a valid e-mail address if: (i) the data collector does not have contact information set forth in subdivisions (i) and (iii) of this subdivision (5)(A), the data collector's primary method of communication with the consumer is by electronic means, the electronic notice does not request or contain a hypertext link to a request that the consumer provide personal information, and the electronic notice conspicuously warns consumers not to provide personal information in response to electronic communications regarding security breaches; or (ii) the notice provided is consistent with the provisions regarding electronic records and signatures for notices as set forth in 15 U.S.C. § 7001; or 3) Telephonic notice, provided that telephonic contact is made directly with each affected consumer, and the telephonic contact is not through a prerecorded message 4) Substitute notice (i) conspicuous posting of the notice on the data collector's website page if the data collector maintains one; and (ii) notification to major statewide and regional media.</p>	<p>Yes;</p>
<p>Virginia</p>	<p>Va. Code § 18.2-186.6 SB 307, Chapter 566</p>	<p>3/11/2008</p>	<p>Undefined</p>	<p>If unencrypted or unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person and causes, or the individual or entity reasonably believes has caused or will cause, identity theft or another fraud to any resident of the Commonwealth, an individual or entity 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 of the security of the system to the Office of the Attorney General and any affected resident of the Commonwealth without unreasonable delay.</p> <p>An individual or entity that maintains computerized data that includes personal information that the individual or entity does not own or license shall notify the owner or licensee of the information of any breach of the security of the system without unreasonable delay following discovery of the breach of the security of the system, if the personal information was accessed and acquired by an unauthorized person or the individual or entity reasonably believes the personal information was accessed and acquired by an unauthorized person.</p>	<p>Notice required by this section may be reasonably delayed to allow the individual or entity to determine the scope of the breach of the security of the system and restore the reasonable integrity of the system. Notice required by this section may be delayed if, after the individual or entity notifies a law-enforcement agency, the law-enforcement agency determines and advises the individual or entity that the notice will impede a criminal or civil investigation, or homeland or national security. Notice shall be made without unreasonable delay after the law-enforcement agency determines that the notification will no longer impede the investigation or jeopardize national or homeland security.</p> <p>An individual or entity shall disclose the breach of the security of the system if encrypted information is accessed and acquired in an unencrypted form, or if the security breach involves a person with access to the encryption key and the individual or entity reasonably believes that such a breach has caused or will cause identity theft or other fraud to any resident of the Commonwealth.</p>	<p>1) Written notice to the last known postal address in the records of the individual or entity 2) Telephone notice; 3) Electronic notice, 4) Substitute Notice a) E-mail notice if the individual or the entity has e-mail addresses for the members of the affected class of residents; b) Conspicuous posting of the notice on the website of the individual or the entity if the individual or the entity maintains a website; c) Notice to major statewide media</p>	<p>Yes</p>

STATE-BY-STATE BREACH NOTIFICATION LAW AND REQUIREMENTS

Washington	Wash. Rev. Code § 19.255.010 SB 6043	7/24/2005	Yes	<p>Any person or business that conducts business in this state 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 this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.</p> <p>Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.</p>	The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.	<p>1) Written notice;</p> <p>2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. Sec 7001;</p> <p>3) Substitute notice</p> <p>(i) E-mail notice when the person or business has an e-mail address for the subject persons;</p> <p>(ii) Conspicuous posting of the notice on the web site page of the person or business, if the person or business maintains one;</p> <p>(iii) notification to major statewide media.</p>	Yes
West Virginia	W.V. Code §§ 46A-2A-101 et seq. SB 340 HB 4551	6/6/2008	Yes	<p>An individual or entity that owns or licenses computerized data that includes personal information shall give notice of 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 this state whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person and that causes, or the individual or entity reasonably believes has caused or will cause, identity theft or other fraud to any resident of this state.</p> <p>An individual or entity that maintains computerized data that includes personal information that the individual or entity does not own or license shall give notice to the owner or licensee of the information of any breach of the security of the system as soon as practicable following discovery, if the personal information was or the entity reasonably believes was accessed and acquired by an unauthorized person.</p>	<p>the notice shall be made without unreasonable delay.</p> <p>An individual or entity that maintains computerized data that includes personal information that the individual or entity does not own or license shall give notice to the owner or licensee of the information of any breach of the security of the system as soon as practicable following discovery, if the personal information was or the entity reasonably believes was accessed and acquired by an unauthorized person.</p>	<p>1) Written notice to the postal address in the records of the individual or entity;</p> <p>2) Telephonic notice;</p> <p>3) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures, set forth in Section 7001, United States Code Title 15, Electronic Signatures in Global and National Commerce Act.</p> <p>4) Substitute notice</p> <p>(i) E-mail notice if the individual or the entity has e-mail addresses for the members of the affected class of residents;</p> <p>(ii) Conspicuous posting of the notice on the website of the individual or the entity if the individual or the entity maintains a website; or</p> <p>(iii) Notice to major statewide media.</p>	Yes

STATE-BY-STATE BREACH NOTIFICATION LAW AND REQUIREMENTS

Wisconsin	Wis. Stat. § 134.98 et seq. SB 164	3/30/2006	No	<p>If an entity whose principal place of business is located in this state or an entity that maintains or licenses personal information in this state knows that personal information in the entity's possession has been acquired by a person whom the entity has not authorized to acquire the personal information.</p> <p>If the entity whose principal place of business is not located in this state knows that personal information pertaining to a resident of this state has been acquired by a person whom the entity has not authorized to acquire the personal information</p> <p>If a person, other than an individual, that stores personal information pertaining to a resident of this state but does not own or license the personal information, knows that the personal information has been acquired by a person whom the person storing the personal information has not authorized to acquire the personal information, and the person storing the personal information has not entered into a contract with the person that owns or licenses the personal information...</p>	<p>The entity shall make reasonable efforts to notify each subject of the personal information. The notice shall indicate the entity knows of the unauthorized acquisition of personal information pertaining to the subject of the personal information.</p> <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>The person storing the personal information shall notify the person that owns or licenses the personal information of the acquisition as soon as practicable.</p>	<p>1) By mail 2) or method the entity has previously employed to communicate with the subject of the personal information 3) Method reasonably calculated to provide actual notice to the subject of the personal information</p>	Yes
Wyoming	Wyo. Stat. § 40-12-501 to - 501 http://legisweb.state.wy.us/2006/introduced/HB0044.pdf	7/1/2007	Undefined	<p>Any person or business that conducts business in this state and that owns or licenses a computerized database that stores personal identifying information shall disclose any breach of the security of the data system following discovery or notification of the breach to any person whose unencrypted personal identifying information whose unencrypted personal identifying information was or is reasonably believed to have been acquired by an unauthorized person.</p> <p>Any person or business that maintains computerized data that includes personal identifying information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data system immediately following discovery if the personal identifying information was or is reasonably believed to have been acquired by an unauthorized person.</p>	The disclosure shall be made without unreasonable delay, consistent with the legitimate needs of law enforcement, or consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.	<p>1) Written notice; 2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. Sec 7001; 3) Telephone notice; 4) If the person or business maintains a written policy for the treatment of personal identifying information in the event of a security breach and notice to affected persons is given as provided in the policy and not unreasonably delayed;</p>	Yes

STATE-BY-STATE BREACH NOTIFICATION LAW AND REQUIREMENTS

District of Columbia	D.C. Code § 28- chapt 38 Subchapter II. Consumer Security Breach Notification § 28-3851. Definitions. § 28-3852. Notification of security breach. § 28-3853. Enforcement.	7/1/2007	Undefined	<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.</p> <p>Any person or entity who maintains, handles, or otherwise possesses computerized or other electronic data that includes personal information that the person or entity does not own shall notify the owner or licensee of the information of any breach of the security of the system in the most expedient time possible following discovery.</p>	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>1) Written notice;</p> <p>2) Electronic notice, if the customer has consented to receipt of electronic notice consistent with the provisions regarding electronic records and signatures set forth in Electronic Signatures in Global and National Commerce Act, approved June 30, 2000 (114 Stat. 641; 15 U.S.C.S. section 7001);</p> <p>3) Substitute notice</p> <p>(i) E-mail notice when the person or business has an e-mail address for the subject persons;</p> <p>(ii) Conspicuous posting of the notice on the website page of the person or business, if the person or business maintains one;</p> <p>(iii) Notice to major local and, if applicable, national media.</p>	Yes
Puerto Rico	10 Laws of Puerto Rico § 4051 et. seq. HB 1184. Law 111	6/1/2006	N/A	<p>Any entity that is the proprietor or custodian of a data bank for commercial use that includes personal information of citizens who reside in Puerto Rico must notify said citizens of any violation of the system's security when the data bank whose security has been violated contains all or part of the personal information file and the same is not protected by a cryptographic code but only by a password.</p> <p>Any entity that as part of their operations resells or provides access to digital data banks that at the same time contain personal information files of citizens must notify the proprietor, custodian or holder of said information of any violation of the system's security that has allowed access to those files to unauthorized persons.</p>	Clients must be notified as expeditiously as possible, taking into consideration the need of law enforcement agencies to secure possible crime scenes and evidence as well as the application of measures needed to restore the system's security. Within a non-extendable term of ten (10) days after the violation of the system's security has been detected, the parties responsible shall inform the Department, which shall make a public announcement of the fact within twenty-four (24) hours after having received the information.	<p>1) Written direct notice to those affected by mail or by authenticated electronic means according to the Digital Signatures Act;</p> <p>2) Substitute notice</p> <p>i) Prominent display of an announcement to that respect at the entities premises, on the web page of the entity, if any, and in any informative flier published and sent through mailing lists both postal and electronic, and</p> <p>ii) a communication to that respect to the media informing of the situation and providing information as to how to contact the entity to allow for better follow-up. When the information is of relevance to a specific professional or commercial sector, the announcement may be made through publications or programming of greater circulation oriented towards that sector.</p>	
Virgin Islands	V.I. Code § 2208	10/17/2005	N/A	<p>Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of the Virgin Islands whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.</p> <p>Any agency that maintains computerized data that includes personal information that the agency does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.</p>	The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.	<p>1) Written notice;</p> <p>2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in section 7001 of Title 15 of the United States Code.</p> <p>3) Substitute notice</p> <p>(i) E-mail notice when the agency has an e-mail address for the subject persons;</p> <p>(ii) Conspicuous posting of the notice on the agency's Web site page, if the agency maintains one;</p> <p>(iii) Notification to major territory-wide media</p>	