



Notice of Security Breach State Laws

Last updated August 21, 2007

Arizona – SB 1338, effective 12/31/2006. Requires notice to consumers of breach in the security of unencrypted, unredacted computerized personal information. No notice if a reasonable investigation determines there is no reasonable likelihood of harm to consumers. If entity complies with federal rules, then it is deemed to be in compliance with Arizona law.

Arkansas – SB 1167, Passed into law in 2005. Now cite as Ark. Code Ann. § 4-110-101 to 108. Effective since 3/31/2005. Requires notice to consumers of breach in the security of unencrypted computerized, personal information and medical information in electronic or physical form. Notice is not required if no reasonable likelihood of harm to consumers. If entity complies with state or federal law that provides greater protection, and at least as thorough disclosure and in compliance with the state or federal law, then deemed in compliance.

California - Civil Code Sec. 1798.80-1798.82, effective July 1, 2003. Requires notice to consumers of breach in the security, confidentiality, or integrity of unencrypted computerized personal information held by a business or a government agency. If person or business has own notification procedures consistent with timing requirements and provides notice in accordance with its policies or if person or business abides by state or federal law provides greater protection and disclosure, then deemed in compliance.

Colorado – Co. Rev. Stat. §6-1-716(1)(a), effective Sept. 1, 2006. Requires notice to consumers of breach in the security of unencrypted, unredacted computerized personal information. Notice given unless investigation determines misuse of information has not occurred or is not reasonably likely to occur. If entity is regulated by state or federal law and maintains procedures pursuant to laws, rules, regulations or guidelines, entity is deemed in compliance.

Connecticut – SB 650, Passed into law 2005, effective January 1, 2006. Now cite as 699 Gen. Stat. Conn. §36a-701. Requires notice of security breach by persons who conduct business in the state and have a breach of the security of unencrypted computerized data, electronic media or electronic files, containing personal information. Notice is not required if the breached entity determines in consultation with federal, state, and local law enforcement agencies that the breach will not likely result in harm to the individuals. Governmental entities not required to provide notice under this section. Entities are also deemed compliant if notification is in compliance with rules or guidelines established by the primary function of the regulator under the Gramm-Leach Bliley Act.

Delaware – HB 116, signed June 28, 2005. Now cite as Del. Code Ann. Title 6 Section 12B-101 to 12-B-106. Requires notice to consumers of breach in the security of unencrypted computerized personal information if the investigation determines that misuse of information about a Delaware resident has occurred or is reasonably likely to occur. If entity is regulated by state or federal law and maintains procedures for a breach pursuant to the laws, rules, regulations, guidances or guidelines established by its primary or functional state or federal regulator, then deemed in compliance with this chapter if entity notifies affected residents in accordance with the maintained procedures when a breach occurs.

District of Columbia – DC Code Sec 28-3851 et seq. Effective January 1, 2007. Requires notice to consumers of breach in the security, confidentiality, or integrity of unencrypted computerized or other electronic personal information held by a business or a government agency. This section does not pertain to person or entity subject to the Gramm-Leach Bliley Act. This section also does not apply to a person or business with its own notification procedures with consistent timing requirements in compliance with notification requirements of this section and the person or business provides notice in accordance with its policies and is reasonably calculated to give actual notice.

Florida – HB 481, Effective July 1, 2005. Now cite as Fla. Stat. Ann. 817.5681 et seq. Requires notice to consumers of breach in the security, confidentiality or integrity of computerized, unencrypted personal information held by a person who conducts business in the state. Notice not required if after appropriate investigation or consultation with law enforcement, person reasonably determined breach has not and will not likely result in harm to individuals. Determination must be documented in writing and maintained for five years. Deemed in compliance if person's own notification procedure is otherwise consistent with the timing requirements of this section, or if notification procedures established by person's primary or functional federal regulator.

Georgia – SB 230, Passed into law in 2005, effective May 6, 2005. Now cite as Ga. Code Ann. 10-1-910 et seq. Covers only data brokers. Requires notice of breach that compromises the security, confidentiality, or integrity of computerized personal information held by a data broker.

Hawaii – HRS Sec 487N et seq. Requires notice when 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. Notice under this section not required by financial institution subject to Federal Interagency Guidance on Response Programs for Unauthorized Access to Consumer Information and Consumer Notice and any health plan or healthcare provider under HIPAA.

Idaho – Id. Code Ann. §28-51-104, effective July 1, 2006. Requires notice to consumers of breach in the security of unencrypted, computerized personal information if after a reasonable investigation, the agency, individual or entity determines that misuse of information of Idaho resident has occurred or is reasonably likely to occur. Notice under this section not required by persons regulated by state or federal law and complies with maintained procedures under that law.

Illinois – HB 1633, Public Act 094-0036, signed June 16, 2005, effective Jan. 1, 2006. Now cite as ILCS Sec. 530/1 et seq. Requires notice to consumers of breach in the security, confidentiality, or integrity of personal information of the system data held by a person or a government agency. Notice under this section not required if entity maintains 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 Act.

Indiana – (government) Act No. 503, Passed into law in 2005, effective June 30, 2006. Now cite as Ind. Code Sec. 4-1-11 et seq. Requires notice to consumers of breach in the security, confidentiality, or integrity of computerized personal information held by a government agency.

(private entities) Ind. Code Sec. 24-2-9 et seq. Requires notice when a data collector knows, should know, or should have known that the unauthorized acquisition of computerized data, including computerized data that has been transferred to another medium, constituting the breach has resulted in or could result in identity deception, ID theft or fraud. Notice not required under this section if entity maintains own disclosure procedures, is under federal USA Patriot Act, Exec. Order 13224, FCRA, Financial Modernization Act, HIPAA or financial institutions that comply with the Federal Interagency Guidance on Response Programs for Unauthorized Access to Member Info and Member Notice.

Kansas – SB 196 will go into effect on Jan. 1, 2007. Now cite as Kansas Stat. 50-7a01, 50-7a02. Requires notice to consumers about a breach in the security of unencrypted, unredacted computerized personal information if investigation determines misuse has occurred or is reasonably likely occur.

Louisiana – SB 205, Act 499, signed July 12, 2005, effective January 1, 2006. Now cite as La. Rev. State. Ann. Sec. 51 3071-3077. Requires notice of a breach of the security, confidentiality, or integrity of unencrypted, computerized, personal information by persons doing business in the state. No notice if, after a reasonable investigation, the data holder determines that there is no reasonable likelihood of harm to customers. Notice not required by financial institutions which are in compliance with federal guidance.

Maine – LD 1671, signed June 10, 2006, effective January 31, 2006. Now cite as Me. Rev. Stat. Ann. 10-21-B-1346 to 1349. Covers only information brokers. Requires notice of a breach of the security, confidentiality, or integrity of unencrypted, computerized, personal information if the personal information has been or is reasonably believed to have been acquired by an unauthorized person. Notice under this section not required by persons regulated by state or federal law and complies with maintained procedures under that law.

Massachusetts – HB 4144 or Public Law 82-2007, effective February 3, 2008. Requires notice of a breach unauthorized acquisition of unencrypted data, or encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality or integrity of the personal information that creates a significant risk of identity theft or fraud. Provide notice to the attorney general, the director of consumer affairs and business and the resident when person or agency who owns or licenses personal information knows or has reason to know of a breach of security or when the person or agency knows or has reason to know that the personal info was acquired or used by an unauthorized person or used for an unauthorized

purpose.

Michigan – SB 209, Passed into law December 2006, effective July 2, 2007. Requires notice of a breach of the security, confidentiality, or integrity of unencrypted, computerized, personal information by persons doing business in the state. Notice under this section not required unless person/agency determines security breach has not or is not likely to cause substantial loss or injury to, or result in ID theft. Does not apply to financial institutions or HIPAA entities.

Minnesota – H.F. 2121, Passed into law 2005, effective January 1, 2006. Now cite as Minn. Stat. 324E.61 et seq. Requires notice of a breach of the security, confidentiality, or integrity of unencrypted, computerized, personal information by persons doing business in the state. Does not apply to financial institutions or HIPAA entities.

Montana – HB 732, Passed into law in 2005, effective March 1, 2006. Now cite as Mont. Code Ann. 31-3-115. Requires notice to consumers of breach in security, confidentiality, or integrity of computerized personal information held by a person or business if the breach causes or is reasonably believed to have caused loss or injury to a Montana resident. Notice under this section not required if entity maintains 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 section.

Nebraska – L.B. 876 passed in 2006. Now cite as Neb. Rev Stat. 87-801 et seq. Requires notice to consumers of a breach in the security of unencrypted, computerized personal information if investigation determines use of information has occurred or is reasonably likely to occur. Deemed in compliance if person's own notification procedure is otherwise consistent with the timing requirements of this section, or if notification procedures established by person's primary or functional federal regulator.

Nevada – SB 347, Passed into law 2005, effective January 1, 2006. Now cite as Nev. Rev. Stat. 607A.010 et seq. Requires notice of breach of the security, confidentiality, or integrity of unencrypted computerized personal information by data collectors, which are defined to include government, business entities and associations who handle, collect, disseminate or otherwise deal with nonpublic personal information. Notice under this section not required if entity maintains 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 section, and entities subject to compliance with the Gramm Leach-Bliley Act.

New Hampshire – HB 1660 FN passed in 2006 and effective starting January 1, 2007. Now cite as NH RS 359-C: 19 et seq. Requires notice of unauthorized acquisition if determined likelihood information has been or will be misused. Notice if determination is that misuse of information has occurred or is reasonably likely to occur or if determination cannot be made. Notice under this section not required if entity maintains 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 section.

New Jersey – A4001/S1914, Passed into law in 2005, effective January 1, 2006. Requires notice of breach of security of unencrypted computerized personal information held by a

business or public entity. No notice if a thorough investigation finds misuse of the information is not reasonably possible. Written documentation of the investigation must be kept for 5 years. Notice under this section not required if entity maintains 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 section.

New York – A4254, A3492, effective December 8, 2005. Now cite as NY Bus. Law Sec. 899-aa. Requires notice of breach of security of computerized unencrypted, or encrypted with acquired encryption key, personal information held by both public and private entities.

North Carolina – SB 1048, effective December 1, 2005. Now cite as N.C. Gen. Stat. 75-65. Requires notice of breach of security of unencrypted and unredacted written, drawn, spoken, visual or electromagnetic personal information, and encrypted personal information with the confidential process or key held by a private business if the breach causes, is reasonably likely to cause, or creates a material risk of harm to residents of North Carolina. Financial institutions subject to compliance with Federal Interagency Guidance on Response Programs for Unauthorized Access to Member Info and Member Notice are exempt.

North Dakota – SB 2251, effective June 1, 2005. Now cite as N.D. Cent. Code 51-30. Requires notice of a breach of the security of unencrypted, computerized, personal information by persons doing business in the state. Includes an expanded list of sensitive personal information, including date of birth, mother's maiden name, employee ID number, and electronic signature. Exception for those financial institutions which are in compliance with federal guidance.

Ohio – HB 104, effective February 15, 2006. Requires notice of breach of the security or confidentiality of computerized personal information, held by a state agency, political subdivision or business is reasonably believed will cause a material risk of identity theft or fraud to a person or property of a resident of Ohio. Notice under this section not required by financial institution, trust company or credit union or any affiliate required by federal law to notify customers of information security breach and is in compliance with federal law.

Oklahoma – HB 2357, effective June 8, 2006. Now cite as Okla. Stat. 74-3113.1. Requires notice of 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. Notice is not required under this section by a state agency, board, commission, or unit or subdivision of government if the entity maintains 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 section.

Oregon – SB 583, effective October 1, 2007. Requires notice when unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information maintained by the person. Notice not required if after an appropriate investigation or after consultation with federal, state or local agencies responsible for law enforcement, the person determines no reasonable likelihood of harm to consumers whose personal info has been acquired has resulted or will result from the breach. Determination must

be in writing and kept for 5 years. Exception for those with own notification procedures under state or federal law providing at least greater protection to personal information and at least as thorough disclosure requirements pursuant to the rules, regulations, procedures, guidance or guidelines established by primary regulator, or state or federal laws, and financial institutions which are in compliance with federal guidance.

Pennsylvania – SB 712, effective June 30, 2006. Now cite as 73 Pa. Cons. Stat. 2303. Requires notice of breach of the security or confidentiality of computerized personal information, held by a state agency, political subdivision or business and is reasonably believed to have been accessed or acquired by an unauthorized person. Notice under this section not required if entity maintains 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 section. Financial institutions subject to compliance with Federal Interagency Guidance on Response Programs for Unauthorized Access to Member Info and Member Notice are exempt.

Rhode Island – H. 6191, effective March 1, 2006. Now cite as RI Gen. Law 11-49.2-3 to 11.49.2-7. Requires notice of a breach of the security, confidentiality or integrity of unencrypted, computerized, personal information by persons and by state agencies if breach poses significant risk of identity theft when unencrypted personal information was, or is reasonably believed to have been acquired by an unauthorized person. No notice is required if after an appropriate investigation or after consultation with relevant federal, state, and local law enforcement agencies determine the breach has not and will not likely result in harm to individuals. Does not apply to HIPAA entities or financial institutions in compliance with Federal Interagency Guidelines. Entities covered by another state or federal law are exempt only if that other law provides greater protection to consumers.

Tennessee – SB 2220, amends Tennessee Code Title 47 Chapter 18, Part 21, effective July 1, 2005. Requires notice of the unauthorized acquisition of unencrypted computerized data that materially compromises the security, confidentiality, or integrity of personal information. Does not apply to persons subject to Title V of the Gramm-Leach-Bliley Act.

Texas – SB 122, effective September 1, 2005. Now cite as Tex. Bus & Com. Code Ann. 4-48-103. Requires notice of a breach of the security, confidentiality, or integrity of unencrypted, computerized, personal information by persons who conduct businesses in the state. Notice under this section not required if entity maintains 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 section.

Utah – SB 69, effective Jan. 1, 2007. Now cite as Utah Code 13-44-101 et seq. Law provides requires notice of a breach of the security of computerized personal information that is not protected by a method that makes the information unusable. Entities covered by another state or federal law are exempt if person notifies each affected Utah resident in accordance with law.

Vermont – Vt. Stat. Tit 9 Sec. 2435, effective in Jan. 1, 2007. Requires notice if investigation reveals misuse of personal information for ID theft or fraud has occurred, or is reasonably likely to occur. Notice is not required if data collector establishes misuse of personal information is not reasonably possible, must provide notice and explanation to the Attorney General or

department of banking, insurance, securities and health care administration in the event data collector is a person/entity licensed with that department. Financial institutions subject to compliance with Federal Interagency Guidance on Response Programs for Unauthorized Access to Member Info and Member Notice are exempt.

Washington – SB 6043, effective July 24, 2005. Now cite as RCW 42.17 et seq. Requires notice of a breach of the security, confidentiality, or integrity of unencrypted, computerized, personal information by persons, businesses and government agencies. Notice is not required when there is a technical breach of the security of the system which does not seem reasonably likely to subject customers to a risk of criminal activity. Notice under this section not required if entity maintains 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 section.

Wisconsin – SB 164, effective March 16, 2006. Now cite as Wis. Stat. 895.507. Law requires notice to the consumer when information is taken in a security breach that is not encrypted, redacted or altered in any manner rendering the information unreadable. This includes DNA and biometric data. Notice not required if the acquisition of personal information does not create a material risk of ID theft or fraud.

Wyoming – SB 53, effective July 1, 2007. Requires notice of the unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal identifying information of an investigation determines misuse of the personal identifying information has occurred or is reasonably likely to occur. Financial institutions under 15 USC 6809 (GLBA) or credit unions under 12 USC 1752 are exempt from providing notice under this section.

Updated 8/22/2007