

Notice of Security Breach State Laws

Last updated January 7, 2009

Alaska – A.S. 45.48.010, effective July 1, 2009. Requires notice to consumers of breach in the security of unencrypted, unredacted personal information in physical or electronic form, or encrypted information where the encryption key may also have been compromised. No notice if a reasonable investigation determines there is no reasonable likelihood of harm to consumers. Written documentation of the investigation must be kept for 5 years. Entities subject to compliance with the Gramm-Leach-Bliley Act are exempt.

Arizona – A.R.S. 44-7501, effective December 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 – Ark. Code Ann. 4-110-101 to 108, effective March 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 it is 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 the person or business has own notification procedures consistent with timing requirements and provides notice in accordance with its policies or if the person or business abides by state or federal law provides greater protection and disclosure, then it is deemed in compliance.

Colorado – Co. Rev. Stat. 6-1-716(1)(a), effective September 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, it is deemed in compliance.

Connecticut – 699 Gen. Stat. Conn. 36a-701, effective January 1, 2006. 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 – Del. Code Ann. Title 6 Section 12B-101 to 12-B-106, effective June 28, 2005. 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 the 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 it is deemed in compliance with this chapter provided it 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 which is reasonably calculated to give actual notice.

Florida – Fla. Stat. Ann. 817.5681 et seq., effective July 1, 2005. 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 determines 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 "maintaining" notification procedures established by person's primary or functional federal regulator.

Georgia – Ga. Code Ann. 10-1-910 et seq., effective May 24, 2007. Covers "information brokers and data collectors". Requires notice of breach that compromises the security, confidentiality, or integrity of computerized personal information held by an info broker or data collector.

Hawaii – HRS Sec 487N-1 et seq., effective January 1, 2007. 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 a financial institution subject to Federal Interagency Guidance on Response Programs for Unauthorized Access to Consumer Information and Consumer Notice or by 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 a person regulated by state or federal law and who complies with procedures under that law.

Illinois – ILCS Sec. 530/1 et seq., effective January 1, 2006. 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 – Ind. Code Sec. 4-1-11 et seq., effective June 30, 2006. 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.

Iowa – Iowa Code Chapter 2007-1154, effective July 1, 2008. Requires notice to consumers of breach in the security of unencrypted, unredacted personal information electronic form. No notice if a reasonable investigation determines there is no reasonable likelihood of harm to consumers. Written documentation of the investigation must be kept for 5 years. Exempted are those with own notification procedures or 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. Entities subject to compliance with the Gramm-Leach-Bliley Act are exempt.

Kansas – Kansas Stat. 50-7a01, 50-7a02, effective January 1, 2007. 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 – La. Rev. State. Ann. Sec. 51 3071-3077, effective January 1, 2006. 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 in compliance with federal guidance.

Maine – Me. Rev. Stat. Ann. 10-21-B-1346 to 1349, effective January 31, 2006. 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 is not required by persons regulated by state or federal law and which complies with procedures under that law.

Massachusetts – 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.

Michigan – 2006-PA-0566, 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 required unless person/agency determines security breach has not or is not likely to cause substantial loss or injury to, or result in identity theft. Does not apply to financial institutions or HIPAA entities.

Minnesota – Minn. Stat. 324E.61 et seq., effective January 1, 2006. 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 – Mont. Code Ann. 31-3-115, effective March 1, 2006. 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 is not required 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.

Nebraska – Neb. Rev. Stat. 87-801 et seq., effective July 16, 2006. Requires notice to consumers of a breach in the security of unencrypted, computerized personal information if an

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 – Nev. Rev. Stat. 607A.010 et seq., effective January 1, 2006. 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 is not required 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, or is subject to compliance with the Gramm-Leach-Bliley Act.

New Hampshire – NH RS 359-C: 19 et seq., effective January 1, 2007. Requires notice of unauthorized acquisition if determined likelihood information has been or will be misused. Notice must be given if there is a determination that misuse of information has occurred or is reasonably likely to occur or if a determination cannot be made. Notice under this section not required 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 or if the entity is a person engaged in trade or commerce under RSA 358-A:3 and maintains notification procedures established by its primary or functional regulator.

New Jersey – NJ Stat 56:8-163, effective July 2, 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 – NY Bus. Law Sec. 899-aa., effective December 8, 2005. 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 – N.C. Gen. Stat. 75-65, effective December 1, 2005. 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 – N.D. Cent. Code 51-30, effective June 1, 2005. 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 – O.R.C. Ann. 1349.19 et seq., effective February 17, 2006. Requires notice of breach of the security or confidentiality of computerized personal information, held by a state agency, political subdivision or business where reasonably believed it will cause a material risk of identity theft or fraud to a person or property of a resident of Ohio. Notice under this section is not required by financial institutions, trust companies or credit unions or any affiliate required by

federal law to notify customers of information security breach and who is in compliance with federal law.

Oklahoma – Okla. Stat. 74-3113.1, effective June 8, 2006. Requires state government agencies to give 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 – O.R.S. 646A.604, 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. Exempted are 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 – 73 Pa. Cons. Stat. 2303, effective June 30, 2006. 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 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 section. Financial institutions subject to compliance with Federal Interagency Guidance on Response Programs for Unauthorized Access to Member Info and Member Notice are exempt.

Puerto Rico – 10 L.P.R.A. 4051 et seq., effective January 5, 2006. Requires notice of breach of the security, confidentiality and integrity of unencrypted personal information, where access has been permitted to unauthorized persons or it is known or reasonably suspected that authorized persons have accessed the information with intent to use it for illegal purposes.

Rhode Island – RI Gen. Law 11-49.2-3 to 11.49.2-7, effective March 1, 2006. 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.

South Carolina – SC Code §1-11-490 et seq., effective January 1, 2009. Requires notice of the security of computerized, unencrypted and unredacted personal information, or encrypted information with a key that has also been compromised, when illegal use of the information has occurred or is reasonably likely to occur or use of the information creates a "material risk of harm" to the consumer. Notice under this section is not required if entity 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 section.

Tennessee – Tenn. Code. Ann. 47-18-21, 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 – Tex. Bus & Com. Code Ann. 4-48-103, effective September 1, 2005. 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 the entity 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 section.

Utah – Utah Code 13-44-101 et seq., effective January 1, 2007. 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 the person notifies each affected Utah resident in accordance with law.

Virgin Islands – 14 V.I.C. 2208 et seq., effective October 17, 2005. Requires notice of a breach of the security, confidentiality, or integrity of unencrypted, computerized, personal information reasonably believed to have been acquired by unauthorized persons. 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.

Virginia – VA Code 18.2-186.6, effective July 1, 2008. Requires notice of any breach of the security of computerized, unencrypted and unredacted personal information, or encrypted information with a key that has also been compromised, if an individual or entity reasonably believes such information has been accessed and acquired by an unauthorized person and has caused or will cause identity theft or other fraud. Notice under this section is not required if an entity 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 section, or if the entity has notification procedures established by a federal regulator. This section does not apply to any entity that is subject to compliance with the Gramm-Leach-Bliley Act.

Vermont – Vt. Stat. Tit 9 Sec. 2435, effective January 1, 2007. Requires notice if investigation reveals misuse of personal information for identity theft or fraud has occurred, or is reasonably likely to occur. Notice is not required if the data collector establishes that 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 – RCW 42.17 et seq., effective July 24, 2005. 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.

West Virginia – WV Code 46A-2A-101 et seq., effective June 26, 2008. Requires notice of any breach of the security of computerized, unencrypted and unredacted personal information, or encrypted information with a key that has also been compromised, reasonably believed to have been accessed and acquired by an unauthorized person and has caused, or will cause, identity theft or other fraud. Financial institutions subject to compliance with Federal Interagency Guidance on Response Programs for Unauthorized Access to Member Info and Member Notice are exempt.

Wisconsin – Wis. Stat. 895.507, effective March 16, 2006. Requires notice to the consumer when personal 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 – W.S. 40-12-501 to 509, 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 subject to the Gramm-Leach-Bliley Act or credit unions under 12 USC §1752 are exempt from providing notice under this section.

Updated 1/7/2009