



Notice of Security Breach State Laws

Last updated June 27, 2006

Arkansas – SB 1167, Passed into law in 2005. Now cite as Ark. Code Ann. § 4-110-101 to 108. Effective since 3/31/2005. Law provides notice to consumers of breach in the security of unencrypted computerized, personal information which is held by a person or business. Notice is not required if no reasonable likelihood of harm to consumers.

Arizona – SB 1338, effective 12/31/2006. Law provides notice to consumers of breach in the security of unencrypted, unredacted computerized personal information when there is a reasonable likelihood of harm to consumers. If entity complies with federal rules, then it is deemed to be in compliance with Arizona law.

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.

Colorado – Co. Rev. Stat. §6-1-716(1)(a); effective Sept. 1, 2006. Law provides notice to consumers of breach in the security of unencrypted, computerized personal information. Notice is not required if there is no reasonable likelihood of harm to consumers.

Connecticut – SB 650, Passed into law 2005, effective January 1, 2006 as 699 Gen. Stat. Conn. §36a-701. Law 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.

Delaware – HB 116, signed June 28, 2005. Law requires notice of a breach of the security, confidentiality or integrity of unencrypted, computerized, personal information by persons doing business in the state. It also covers sensitive personal information including medical information. Violations trigger triple damages plus attorney's fees.

Florida – HB 481, signed June 14, 2005, Chapter 2005-229. Effective July 1, 2005. Requires notice to consumers of material breach in the security, confidentiality or integrity of computerized, unencrypted personal information held by a person who

conducts business in the state. Time limits for the notice to be given and penalties if notice is not given on time. Penalties do not apply to government agencies.

Georgia – SB 230, Passed into law in 2005, effective May 6, 2005. Requires notice of breach that compromises the security, confidentiality, or integrity of computerized personal information held by a data broker.

Idaho – Id. Code Ann. §28-51-104, effective July 1, 2006. Law provides notice to consumers of breach in the security of unencrypted, computerized personal information. To be required to notify, the security breach must result in a reasonable likelihood of identity theft.

Illinois – HB 1633, Public Act 094-0036, signed June 16, 2005, effective Jan. 1, 2006. Requires notice to consumers of breach in the security, confidentiality, or integrity of personal information in system data held by a person or a government agency.

Indiana – Act No. 503, Passed into law in 2005, effective June 30, 2006. Law provides notice to consumers of breach in the security, confidentiality, or integrity of computerized personal information held by a government agency.

Kansas – SB 196 will go into effect on Jan. 1, 2007. The law provides notice to consumers about a breach in the security of unencrypted, unredacted computerized personal information. To be required to notify, there must be a reasonable likelihood of harm to consumers.

Louisiana – SB 205, Act 499, signed July 12, 2005, effective January 1, 2006, or such later time if the Attorney General completes regulations. 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. Further exemption for those financial institutions which are in compliance with federal guidance. Authorizes civil actions to recover actual damages.

Maine – LD 1671, signed June 10, 2006, effective January 31, 2006. Covers only information brokers. Requires notice of a breach of the security, confidentiality, or integrity of unencrypted, computerized, personal information to residents of the state. Provides civil penalties for violations.

Minnesota – H.F. 2121, Passed into law 2005, 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 – HB 732, Passed into law in 2005, effective March 1, 2006. Law provides 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.

Nebraska – L.B. 876 passed in 2006. Law provides notice to consumers of a breach in the security of unencrypted, computerized personal information. To be required to notify the consumer of the security breach, there must be a reasonable likelihood that the information will be used in a way that will harm the consumer.

Nevada – SB 347, Passed into law 2005, 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.

New Hampshire – HB 1660 FN passed in 2006 and effective starting January 1, 2007. Law provides notice to consumers of a breach in the security of unencrypted, computerized personal information. If there is a reasonable likelihood of harm to the consumer, entity must inform the consumer of the breach.

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.

New York – A4254, A3492, Passed into law in 2005, effective 120 days after September 20, 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. The State Attorney General, the State Consumer Protection Board and the Office of Cyber Security and Critical Infrastructure Coordination must also be notified of the breach of security to protect the residents of New York. Authorizes Attorney General to bring actions on behalf of affected residents.

North Carolina – SB 1048, Passed into law in 2005, 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. Provides civil and criminal penalties for violations.

North Dakota – SB 2251, Passed into law in 2005, North Dakota Century Code Chapter 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 – HB 104, Signed into law November 17, 2005, 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 to have caused or reasonably is believed will cause a material risk of identity theft or other fraud to an Ohio resident. Personal information includes information that describes anything about a person, including actions or certain personal characteristics, and can be retrieved from a system by a name, identifying number, symbol, or other identifier.

Pennsylvania – SB 712, Signed into law December 22, 2005, 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 is reasonably believed to have caused or will cause loss or injury to any Pennsylvania resident. Personal information includes information accessed and acquired in unencrypted form, if the security breach is linked to a breach of the security of the encryption or if the breach involved a person with access to the encryption key. Exception for those financial institutions which are in compliance with federal guidance.

Rhode Island – H. 6191, enacted July 10, 2005, 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. Does not apply to HIPAA entities. Entities covered by another state or federal law are exempt only if that other law provides greater protection to consumers.

Tennessee – SB 2220, Passed into law in 2005, amends Tennessee Code Title 47 Chapter 18, Part 21, effective July 1, 2005. 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 persons subject to Title V of the Gramm-Leach-Bliley Act (financial institutions).

Texas – SB 122, Passed into law in 2005, 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. Authorizes Attorney General to seek civil penalties for violations.

Utah – SB 69 will go into effect on Jan. 1, 2007. 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. Those entities regulated by other state or federal laws are exempt from this one. If there is a reasonable likelihood of harm to the consumer, then the entity must inform the consumer of the breach.

Washington – SB 6043, Signed May 10, 2005, effective in 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.

Imposes civil liability for damages caused by failure to give notice as required.

Wisconsin – SB 164. 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. The entity need only provide notice if it knows that personal information has been acquired by an unauthorized person. And there is a material risk of identity theft or fraud.

Prepared by:
Gail Hillebrand
West Coast Office
Consumers Union of U.S., Inc.
415 431-6747