

**SUMMARY OF STATE LAWS REQUIRING NOTIFICATION OF A DATABASE SECURITY BREACH
(AS OF OCTOBER 1, 2008)**

STATE	LEGISLATION	SECTION	EFFECTIVE	SUMMARY
Alabama	NO	--		
Alaska	YES	Alaska Stat. §§ 45.48.010 et seq.	July 1, 2009	<p>Requires a person that conducts business in Alaska and owns or licenses unencrypted or unredacted personal information, or encrypted personal information where the key has been accessed or acquired, in any form to disclose a breach of security of an information system.</p> <p>Notice is not required if after an investigation and notice to the State Attorney General the person determines that there is not reasonably likelihood that harm has resulted or will result to the affected individuals.</p> <p>Delayed notice permitted if consistent with law enforcement needs or measures necessary to determine the scope of the breach and restore the reasonable integrity of the information system.</p> <p>Substitute notice procedures permitted if cost exceeds \$150,000, more than 300,000 persons must be notified or insufficient contact information for notice.</p> <p>If more than 1,000 Alaska residents must be notified, the person must notify nationwide consumer reporting agencies of the timing, distribution and content of notices. Persons subject to the Gramm-Leach-Bliley Act are exempt from this requirement.</p>
Arizona	YES	Ariz. Rev. Stat. § 44-7501	December 31, 2006	<p>Requires a person that conducts business in Arizona and owns or licenses unencrypted computerized data to disclose after an investigation any incident of unauthorized acquisition and access to unencrypted or unredacted personal information to affected individuals.</p> <p>No notice is required if after an investigation the person determines that a breach has not occurred or is not reasonably likely to occur.</p> <p>Delayed notice permitted if consistent with law enforcement needs or measures necessary to determine the nature and scope of breach, identify affected individuals or restore the reasonable integrity of the data system.</p> <p>Substitute notice procedures permitted if cost exceeds \$50,000,</p>

**SUMMARY OF STATE LAWS REQUIRING NOTIFICATION OF A DATABASE SECURITY BREACH
(AS OF OCTOBER 1, 2008)**

STATE	LEGISLATION	SECTION	EFFECTIVE	SUMMARY
				<p>more than 100,000 persons must be notified or insufficient contact information for notice. Exempts persons subject to Gramm-Leach-Bliley Act or that comply with notification requirements or security breach procedures of their primary or functional regulator.</p>
Arkansas	YES	Ark. Code Ann. §§ 4-110-101 et seq.	August 12, 2005	<p>Requires a person that acquires, owns or licenses computerized data to disclose any breach of security to state residents whose unencrypted personal information (including medical information) was, or is reasonably believed to have been, acquired by an unauthorized person. No notice required if after investigation the person determines there is no reasonable likelihood of harm. Delayed notice permitted if consistent with law enforcement needs or measures necessary to determine scope of the breach and restore integrity of system. Substitute notice procedures permitted if cost exceeds \$250,000 or more than 500,000 persons are affected.</p>
California	YES	Cal. Civ. Code §§ 1798.29, 1798.80 et seq.	July 1, 2003; amendment effective January 1, 2008	<p>Requires a person that conducts business in California and that owns, licenses or maintains computerized data to disclose a security breach to residents whose unencrypted personal information (including medical and health insurance information) was, or is reasonably believed to have been, acquired by an unauthorized person. Delayed notice permitted if consistent with law enforcement needs or measures necessary to determine scope of the breach and restore integrity of system. Substitute notice procedures permitted if cost exceeds \$250,000 or more than 500,000 persons are affected.</p>
Colorado	YES	Col. Rev. Stat. § 6-1-716	September 1, 2006	<p>Requires a person that conducts business in Colorado and owns or licenses computerized data to conduct a prompt investigation when it becomes aware of a breach of security of the system to determine the likelihood that unencrypted, unredacted or otherwise readable</p>

**SUMMARY OF STATE LAWS REQUIRING NOTIFICATION OF A DATABASE SECURITY BREACH
(AS OF OCTOBER 1, 2008)**

STATE	LEGISLATION	SECTION	EFFECTIVE	SUMMARY
				<p>personal information about a Colorado resident has been or will be misused. Notice must be given to Colorado residents unless the investigation determines the misuse of information has not occurred and is not reasonably likely to occur.</p> <p>Delayed notice permitted if consistent with law enforcement needs or measures necessary to determine the scope of the breach and to restore reasonable integrity of the system.</p> <p>Substitute notice procedures permitted if costs exceed \$250,000, more than 250,000 residents are affected or the person has insufficient contact information to provide notice.</p> <p>Exempts persons regulated by state or federal law that maintain procedures as required by their primary or functional regulator.</p> <p>If more than 1,000 Colorado residents must be notified, the person must notify nationwide consumer reporting agencies of the date of notice and number of residents to be notified.</p>
Connecticut	YES	Conn. Gen. Stat. § 36a-701b	January 1, 2006	<p>Requires a person that owns, licenses or maintains computerized data to disclose any breach of security to state residents whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.</p> <p>No notice required if after an investigation and consultation with law enforcement the person determines there is no reasonable likelihood of harm.</p> <p>Delayed notice permitted if consistent with law enforcement needs or measures necessary to determine scope of the breach and restore integrity of system.</p> <p>Substitute notice procedures permitted if cost exceeds \$250,000 or more than 500,000 persons are affected.</p>
Delaware	YES	Del. Code Ann. Tit. 6, §§ 12B-101 et seq.	June 28, 2005	<p>Requires a person that conducts business in the state and that owns or licenses computerized data conduct a reasonable and prompt investigation when it becomes aware of a breach of security of the system to determine the likelihood that unencrypted personal information about a Delaware resident has been or will be misused.</p>

**SUMMARY OF STATE LAWS REQUIRING NOTIFICATION OF A DATABASE SECURITY BREACH
(AS OF OCTOBER 1, 2008)**

STATE	LEGISLATION	SECTION	EFFECTIVE	SUMMARY
				<p>If the investigation determines the misuse of information has occurred or is reasonably likely to occur, notice must be given as soon as possible to the affected Delaware resident.</p> <p>Delayed notice permitted if consistent with law enforcement needs or measures necessary to determine scope of the breach and restore integrity of system.</p> <p>Substitute notice procedures permitted if cost exceeds \$75,000 or more than 1,000 persons are affected.</p> <p>Exempts persons regulated by state or federal law that maintain procedures for a breach of the security of the system pursuant to the requirements established by its primary or functional regulator.</p>
District of Columbia	YES	D.C. Code §§ 28-3851 et seq.	July 1, 2007	<p>Requires a person that conducts business in the District that owns or licenses computerized data that includes personal information disclose a breach of the security of the system to any D.C. resident whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person.</p> <p>Written or electronic notice must be made in the most expedient time possible, without unreasonable delay, and consistent with the needs of law enforcement.</p> <p>Substitute notice procedures permitted if cost exceeds \$50,000 or more than 100,000 persons are affected, or the business does not have sufficient contact information.</p> <p>If more than 1,000 persons must be notified at one time, the business must notify the nationwide consumer reporting agencies of the timing, distribution and content of the notice.</p> <p>Exempts persons that comply with the breach notification provisions of the Gramm-Leach-Bliley Act or that maintain their own notification procedures consistent with the D.C. act.</p>
Florida	YES	Fla. Stat. ch. 817.5681	July 1, 2005	<p>Requires a person that conducts business in the state and that maintains computerized data in a system that includes personal information disclose a breach of the security of the system to any Florida resident whose unencrypted personal information was or is</p>

**SUMMARY OF STATE LAWS REQUIRING NOTIFICATION OF A DATABASE SECURITY BREACH
(AS OF OCTOBER 1, 2008)**

STATE	LEGISLATION	SECTION	EFFECTIVE	SUMMARY
				<p>reasonably believed to have been acquired by an unauthorized person.</p> <p>No notice required if after an investigation or consultation with law enforcement the person determines there is no reasonable likelihood of harm.</p> <p>Delayed notice permitted if consistent with law enforcement needs or measures necessary to determine scope of the breach and restore integrity of system.</p> <p>Substitute notice procedures permitted if cost exceeds \$250,000 or more than 500,000 persons are affected.</p>
Georgia	YES	Ga. Code Ann. §§ 10-1-910 et seq.	May 5, 2005	<p>Requires an “information broker” that maintains computerized data to give notice of any breach of security to state residents whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.</p> <p>“Information broker” is a person or entity who collects information on individuals for the primary purpose of furnishing that information to third parties.</p> <p>Delayed notice permitted if consistent with law enforcement needs or measures necessary to determine scope of the breach and restore integrity, security and confidentiality of system.</p> <p>Substitute notice procedures permitted if cost exceeds \$50,000 or more than 100,000 persons are affected.</p>
Hawaii	YES	Haw. Rev. Stat. §§ 487N-1 et seq.	January 1, 2007	<p>Requires any business that owns, licenses, maintains or possesses personal information of state residents in unencrypted and unredacted records or data or any business conducting business in Hawaii that owns or licenses personal information to provide notice of a security breach to the affected person where illegal use of the information has occurred or is reasonably likely to occur or that creates a material risk of harm to a person.</p> <p>Delayed notice permitted if consistent with law enforcement needs or necessary to determine sufficient contact information, scope of the breach and restore the reasonable integrity, security and</p>

**SUMMARY OF STATE LAWS REQUIRING NOTIFICATION OF A DATABASE SECURITY BREACH
(AS OF OCTOBER 1, 2008)**

STATE	LEGISLATION	SECTION	EFFECTIVE	SUMMARY
				<p>confidentiality of the data system.</p> <p>Substitute notice procedures permitted if cost exceeds \$250,000, more than 500,000 persons must be notified or insufficient contact information or unable to identify particular affected persons, as to the persons for whom there is insufficient contact information or who cannot be identified.</p> <p>If more than 1,000 persons must be notified at one time, the business must notify the State office of consumer protection and the nationwide consumer reporting agencies of the timing, distribution and content of the notice.</p> <p>Exempts financial institutions in compliance with the federal banking agencies' guidance issued on March 7, 2005.</p>
Idaho	YES	Idaho Code §§ 28-51-104 et seq.	July 1, 2006	<p>Requires that a person conducting business in the state that owns or licenses computerized data that includes personal information disclose a breach of the security of the computerized data system to any Idaho resident whose unencrypted personal information was or is reasonably believed to have been misused. Notice is not required if after reasonable and prompt investigation the person determines there is no reasonable likelihood the personal information has been or will be misused.</p> <p>Delayed notice permitted if consistent with law enforcement needs or measures necessary to determine scope of the breach, identify individuals affected and restore the reasonable integrity of system.</p> <p>Substitute notice procedures permitted if cost exceeds \$25,000 or more than 50,000 persons are affected.</p> <p>Exempts persons regulated by state or federal law that maintain procedures for a breach of the security of the system pursuant to the requirements established by its primary regulator.</p>
Illinois	YES	815 Ill. Comp. Stat. 530/5 et seq.	January 1, 2006	<p>Requires a "data collector" that owns or licenses personal information disclose a breach of the security of the computerized system data to any Illinois resident whose unencrypted personal information is compromised.</p>

**SUMMARY OF STATE LAWS REQUIRING NOTIFICATION OF A DATABASE SECURITY BREACH
(AS OF OCTOBER 1, 2008)**

STATE	LEGISLATION	SECTION	EFFECTIVE	SUMMARY
				<p>“Data collector” includes, but not limited to, privately and publicly held corporations, financial institutions and any other entity that, for any purpose, handles, collects, disseminates, or otherwise deals with nonpublic personal information.</p> <p>Delayed notice permitted if consistent with law enforcement needs or measures necessary to determine scope of the breach and restore integrity, security and confidentiality of system.</p> <p>Substitute notice procedures permitted if cost exceeds \$250,000 or more than 500,000 persons are affected.</p>
Indiana	YES	Ind. Code § 24-4.9	July 1, 2006	<p>Requires a “data base owner” to disclose a breach of the security of a system to any Indiana resident whose unencrypted personal information was or may have been acquired by an unauthorized person or whose encrypted personal information was or may have been acquired by an unauthorized person with access to the encryption key, if the data base owner knows, should know or should have known the unauthorized acquisition has resulted or could result in identity deception, identity theft, or fraud affecting the Indiana resident.</p> <p>Delayed notice permitted if consistent with law enforcement needs, necessary to discover the scope of the breach or to restore integrity of the computer system.</p> <p>Substitute notice procedures permitted if cost exceeds \$250,000 or more than 500,000 persons are affected.</p> <p>If more than 1,000 persons must be notified, the data base owner must notify the nationwide consumer reporting agencies.</p> <p>Exempts financial institutions in compliance with the federal banking agencies’ guidance issued on March 7, 2005. Also exempts entities subject to certain other federal laws.</p>
Iowa	YES	Iowa Code §§ 715C.1 et seq.	July 1, 2008	<p>Requires any person that owns or licenses computerized data that includes a resident’s personal information used in the course of the person’s business, vocation, occupation or volunteer activities and subject to an unauthorized acquisition that</p>

**SUMMARY OF STATE LAWS REQUIRING NOTIFICATION OF A DATABASE SECURITY BREACH
(AS OF OCTOBER 1, 2008)**

STATE	LEGISLATION	SECTION	EFFECTIVE	SUMMARY
				<p>compromises the security, confidentiality or integrity of the information must provide notice to the state resident. Notice not required if after an appropriate investigation or after consulting with law enforcement, person determines no reasonable likelihood of financial harm to the consumers has resulted or will result from the breach.</p> <p>Delayed notice permitted if consistent with law enforcement needs, necessary to determine contact information for affected consumers, scope of the breach, and restore the reasonable integrity, security, and confidentiality of the data.</p> <p>Substitute notice procedures permitted if cost exceeds \$250,000, more than 350,000 affected persons, or insufficient contact information for affected consumers.</p> <p>Requires specified information to be provided in notices.</p> <p>Exempts persons who comply with a state or federal law or requirements of primary or functional regulator that provide greater protection to personal information and at least as thorough disclosure requirements. Exempts persons subject to and who comply with regulations under the Gramm-Leach-Bliley Act.</p>
Kansas	YES	Kan. Stat. Ann. §§ 50-7a01 et seq.	July 1, 2006	<p>Requires a person that conducts business in the state that owns or licenses computerized data that includes personal information to disclose a breach to any Kansas resident after an investigation determines misuse of unencrypted or unredacted personal information has occurred or is reasonably likely to occur.</p> <p>Delayed notice permitted if consistent with law enforcement needs or measures necessary to determine the scope of the breach and restore the integrity of the system.</p> <p>Substitute notice procedures permitted if cost exceeds \$100,000, more than 5,000 persons are affected or the person does not have sufficient contact information to provide notice.</p>

**SUMMARY OF STATE LAWS REQUIRING NOTIFICATION OF A DATABASE SECURITY BREACH
(AS OF OCTOBER 1, 2008)**

STATE	LEGISLATION	SECTION	EFFECTIVE	SUMMARY
				Exempts persons regulated by state or federal law that maintain procedures as required by their primary or functional regulator. If more than 1,000 persons must be notified at one time, the person must notify the nationwide consumer reporting agencies of the timing, distribution and content of the notices.
Kentucky	NO	--		
Louisiana	YES	La. Rev. Stat. Ann. §§ 3071 et seq.; La. Admin. Code tit. 16, § 701	January 1, 2006	Requires a person that conducts business in the state or owns or licenses computerized data that includes personal information disclose a breach of the security of the system to any Louisiana resident whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. Notice is not required if after reasonable investigation the person determines there is no reasonable likelihood of harm to customers. Delayed notice permitted if consistent with law enforcement needs or measures necessary to determine scope of the breach, prevent further disclosures and restore integrity of system. Substitute notice procedures permitted if cost exceeds \$250,000 or more than 500,000 persons are affected. Exempts financial institutions that are subject to and in compliance with the federal banking agencies' guidance issued on March 7, 2005. When notice is given to Louisiana residents, regulations require that written notice be provided to the Attorney General's Office within 10 days of distribution of the notice to Louisiana citizens, including the names of all affected Louisiana citizens.
Maine	YES	Me. Rev. Stat. Ann. tit. 10, §§ 1346 et seq.	January 31, 2006; January 31, 2007 with respect to persons other than	Requires an "information broker" that maintains computerized data to disclose after an investigation any breach of the security of the system to state residents whose unencrypted or unredacted personal information has been or is reasonably believed to have been acquired by an unauthorized person. Requires any other person who maintains computerized data to

**SUMMARY OF STATE LAWS REQUIRING NOTIFICATION OF A DATABASE SECURITY BREACH
(AS OF OCTOBER 1, 2008)**

STATE	LEGISLATION	SECTION	EFFECTIVE	SUMMARY
			information brokers	<p>disclose after an investigation any breach of the security of the system to state residents whose unencrypted or unredacted personal information has been or it is reasonably possible will be misused. "Information broker" is a person who, for monetary fees or dues, engages in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring or communicating information concerning individuals for the primary purpose of furnishing personal information to nonaffiliated third parties. Delayed notice permitted if consistent with law enforcement needs or measures necessary to determine scope of the breach and restore integrity, security and confidentiality of data in the system. Substitute notice procedures permitted if cost exceeds \$5,000, more than 1,000 persons are affected or insufficient contact information for written or electronic notice. If more than 1,000 persons must be notified, the person must notify the nationwide consumer reporting agencies and include the date of the breach, estimated number of persons affected, if known, and the date persons were/will be notified of the breach.</p>
Maryland	YES	Md. Code §§ 14-3501 et seq.	January 1, 2008	<p>Requires any other person who maintains computerized data to disclose after an investigation any breach of the security of the system to state residents whose unencrypted or unredacted personal information has been or is reasonably possible that it will be misused. Advance notice is to be provided to the Attorney General. Delayed notice permitted if consistent with law enforcement needs or measures necessary to determine scope of the breach and restore integrity, security and confidentiality of data in the system. Substitute notice permitted if cost exceeds \$100,000, more than 175,000 persons are affected or there is insufficient contact information for written, telephonic, or electronic notice. If more than 1,000 residents must be notified at one time, the person must notify the Office of Consumer Protection and the nationwide consumer reporting agencies of the timing, distribution</p>

**SUMMARY OF STATE LAWS REQUIRING NOTIFICATION OF A DATABASE SECURITY BREACH
(AS OF OCTOBER 1, 2008)**

STATE	LEGISLATION	SECTION	EFFECTIVE	SUMMARY
				<p>and number of notices. Exempts businesses that comply with rules, regulations, procedures, or guidelines established by the primary or functional federal or State regulator of the business, the Gramm-Leach-Bliley Act and other federal guidelines.</p>
Massachusetts	YES	Mass. Gen. Laws ch. 93H, §§ 1 et seq.		<p>Requires any person or agency that owns or licenses data that includes personal information provide notice to any Massachusetts resident, the Attorney General, and the Director of Consumer Affairs and Business Regulation, when it knows or has reason to know of the unauthorized acquisition of unauthorized use of unencrypted data or encrypted data and key maintained by the person that creates a substantial risk of identity theft or fraud against a state resident. Notice is to contain information about how to request credit freeze and the right to obtain a police report. Delayed notice permitted if consistent with law enforcement needs. Substitute notice procedures permitted if cost exceeds \$250,000 or more than 500,000 persons are affected. Exempts persons that maintain procedures for a breach of security pursuant to requirements of federal laws, so long as notice is provided to the Attorney General and Director of Consumer Affairs and Business Regulation. Notice to consumer reporting agencies required upon direction by Director of Consumer Affairs and Business Regulation.</p>
Michigan	YES	Mich. Comp. Laws §§ 445.63 et seq.	July 2, 2007	<p>Requires a person that owns or licenses data in a database that includes personal information disclose any breach of security to any state resident whose unencrypted and unredacted personal information was accessed and acquired by an unauthorized person, or whose encrypted information was accessed and acquired by a person with unauthorized access to the encryption key, unless the person determines the breach has not and is not likely to cause substantial loss or injury or identity theft to state residents.</p>

**SUMMARY OF STATE LAWS REQUIRING NOTIFICATION OF A DATABASE SECURITY BREACH
(AS OF OCTOBER 1, 2008)**

STATE	LEGISLATION	SECTION	EFFECTIVE	SUMMARY
				<p>Delayed notice permitted if consistent with law enforcement needs or measures necessary to determine scope of the breach and restore integrity of system.</p> <p>Substitute notice procedures permitted if cost exceeds \$250,000 or more than 500,000 persons are affected.</p> <p>The act specifically exempts financial institutions, as defined in Title V of the GLBA and entities subject to HIPAA.</p> <p>If more than 1,000 Michigan residents must be notified at one time, the person must notify the nationwide consumer reporting agencies of the timing and number of notices.</p>
Minnesota	YES	Minn. Stat. §§ 325E.61, 325E.64	January 1, 2006	<p>Requires a person that conducts business in Minnesota and that owns or licenses data that includes personal information disclose any breach of security to any state resident whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person.</p> <p>Delayed notice permitted if consistent with law enforcement needs or measures necessary to determine scope of the breach, identify individuals affected and restore integrity of system.</p> <p>Substitute notice procedures permitted if cost exceeds \$250,000 or more than 500,000 persons are affected.</p> <p>The act specifically exempts financial institutions, as defined in Title V of the GLBA and entities subject to HIPAA.</p> <p>If more than 500 persons must be notified at one time, within 48 hours the person must notify the nationwide consumer reporting agencies of the timing, distribution and content of the notices.</p> <p>Effective August 1, 2007, any person or entity conducting business in Minnesota that accepts access devices, such as credit, debit, or stored value cards, in connection with a transaction must not retain the card security code data or the full contents of any track of magnetic stripe data, subsequent to the authorization of the transaction and may not retain PIN data subsequent to 48 hours after authorization of the transaction.</p>

**SUMMARY OF STATE LAWS REQUIRING NOTIFICATION OF A DATABASE SECURITY BREACH
(AS OF OCTOBER 1, 2008)**

STATE	LEGISLATION	SECTION	EFFECTIVE	SUMMARY
				If that provision is violated after August 1, 2008, and a security breach occurs, the person or entity is liable for damages to the financial institution that issued the access device. It shall reimburse the financial institution for its costs in undertaking actions as a result of the breach in order to protect cardholder information or to continue to provide services to cardholders.
Mississippi	NO	--		
Missouri	NO	--		
Montana	YES	Mont. Code Ann. § 30-14-1704	March 1, 2006	Requires a person that conducts business in Montana that owns, licenses, or maintains computerized data disclose any breach of security to any state resident whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person and which causes or is reasonably believed to cause loss or injury. Delayed notice permitted if consistent with law enforcement needs or measures necessary to determine scope of the breach and restore integrity of system. Substitute notice procedures permitted if cost exceeds \$250,000 or more than 500,000 persons are affected. If a person that discloses a breach suggests, indicates or implies the individual may obtain a copy of his or her credit report from a consumer reporting agency, the person must coordinate with the consumer reporting agency as to the notice.
Nebraska	YES	Neb. Rev. Stat. §§ 87-801 et seq.	July 13, 2006	Requires that a person that owns or licenses computerized data that includes personal information disclose a breach of the security of system data to any Nebraska resident after an investigation determines use of unencrypted, unredacted or otherwise readable personal information has occurred or is reasonably likely to occur. Delayed notice permitted if consistent with law enforcement needs or measures necessary to determine scope of the breach and restore integrity of the system. Substitute notice procedures permitted if cost exceeds \$75,000,

**SUMMARY OF STATE LAWS REQUIRING NOTIFICATION OF A DATABASE SECURITY BREACH
(AS OF OCTOBER 1, 2008)**

STATE	LEGISLATION	SECTION	EFFECTIVE	SUMMARY
				<p>more than 100,000 Nebraska residents are affected or insufficient contact information to provide notice. Exempts persons regulated by state or federal law that maintain procedures for a breach of security pursuant to requirements of their primary or functional regulator.</p>
Nevada	YES	Nev. Rev. Stat. §§603A.020 et seq.	January 1, 2006	<p>Requires a “data collector” that owns or licenses computerized data that includes personal information disclose a material breach of the security of the system data to any Nevada resident whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. “Data collector” includes any corporation, financial institution or other business entity that handles, collects, disseminates or otherwise deals with nonpublic personal information. Delayed notice permitted if consistent with law enforcement needs or measures necessary to determine scope of the breach and restore integrity of system. Substitute notice procedures permitted if cost exceeds \$250,000 or more than 500,000 persons are affected. Exempts institutions subject to the GLBA. If more than 1,000 persons must be notified, the person must notify the nationwide consumer reporting agencies of the timing, distribution and content of the notices.</p>
New Hampshire	YES	N.H. Rev. Stat. Ann. §§ 359-C:19 et seq.	January 1, 2007	<p>Requires a person doing business in New Hampshire who owns or licenses computerized data, when it becomes aware of a security breach, to determine the likelihood that unencrypted personal information has been or will be misused. If misuse has occurred or is reasonably likely to occur, or if the determination cannot be made, the person shall notify the affected individuals. Delayed notice is permitted if notification would impede a criminal investigation or jeopardize national or homeland security. Substitute notice procedures permitted if the cost of providing notice would exceed \$5,000, the affected class exceeds 1,000, or</p>

SUMMARY OF STATE LAWS REQUIRING NOTIFICATION OF A DATABASE SECURITY BREACH

(AS OF OCTOBER 1, 2008)

STATE	LEGISLATION	SECTION	EFFECTIVE	SUMMARY
				<p>the person does not have sufficient contact information or consent to make written, electronic or telephonic notice or notice according to the person's internal procedures.</p> <p>Financial institutions must notify their primary regulator of the timing and distribution of the notices. All other persons must notify the New Hampshire attorney general's office.</p> <p>If a person must notify more than 1,000 consumers, the person must notify all nationwide consumer reporting agencies of the timing, distribution and content of the notices.</p>
New Jersey	YES	N.J. Stat. Ann. §§ 56:8-161 et seq.	January 1, 2006	<p>Requires a business that conducts business in the state that maintains computerized records that include personal information disclose a breach of the security of the system to any New Jersey resident whose unencrypted personal information was or is reasonably believed to have been accessed by an unauthorized person.</p> <p>Notice is not required if the business establishes that misuse of the information is not reasonably possible.</p> <p>Delayed notice permitted if consistent with law enforcement needs or measures necessary to determine scope of the breach and restore integrity of system.</p> <p>Substitute notice procedures permitted if cost exceeds \$250,000 or more than 500,000 persons are affected.</p> <p>The business must report the breach of security and any information pertaining to the breach to the Division of State Police in the Department of Law and Public Safety prior to notifying customers.</p> <p>If more than 1,000 consumers must be notified, the business must notify the nationwide consumer reporting agencies of the timing, distribution and content of the notices.</p>

**SUMMARY OF STATE LAWS REQUIRING NOTIFICATION OF A DATABASE SECURITY BREACH
(AS OF OCTOBER 1, 2008)**

STATE	LEGISLATION	SECTION	EFFECTIVE	SUMMARY
New Mexico	No	--		
New York	YES	N.Y. Gen. Bus. Law § 899-aa	December 7, 2005	<p>Requires a person that conducts business in the state and that owns or licenses computerized data to provide notice of any breach of the security of the system to any New York resident whose unencrypted private information was or is reasonably believed to have been acquired by an unauthorized person.</p> <p>Delayed notice permitted if consistent with law enforcement needs or measures necessary to determine scope of the breach and restore integrity of system.</p> <p>Substitute notice procedures permitted if cost exceeds \$250,000 or more than 500,000 persons are affected.</p> <p>If more than 5,000 New York residents must be notified, the person must notify consumer reporting agencies of the timing, distribution and content of the notice and the approximate number of affected persons.</p> <p>The person must notify the State Attorney General, the Consumer Protection Board and the State Office of Cyber Security and Critical Infrastructure Coordination of the timing, distribution and content of the notice and the approximate number of affected persons.</p>

**SUMMARY OF STATE LAWS REQUIRING NOTIFICATION OF A DATABASE SECURITY BREACH
(AS OF OCTOBER 1, 2008)**

STATE	LEGISLATION	SECTION	EFFECTIVE	SUMMARY
North Carolina	YES	N.C. Gen. Stat. § 75-65	December 1, 2005	<p>Requires that a business that owns or licenses personal information of residents of North Carolina or that conducts business in the state and owns or licenses personal information of consumers in any form (computerized, paper or otherwise) disclose a breach of the security of the system to any affected person whose personal information was acquired by an unauthorized person and where illegal use of the personal information has occurred or is reasonably likely to occur or creates a material risk of harm.</p> <p>Delayed notice permitted if consistent with law enforcement needs or measures necessary to determine sufficient contact information, determine scope of the breach and restore integrity, security and confidentiality of system.</p> <p>Substitute notice procedures permitted if cost exceeds \$250,000 or more than 500,000 persons are affected.</p> <p>Exempts financial institutions that are subject to and in compliance with the federal banking agencies' guidance issued on March 7, 2005.</p> <p>If more than 1,000 consumers must be notified, the person must notify the Consumer Protection Division of the Attorney General's Office and the nationwide consumer reporting agencies of the timing, distribution and content of the notice.</p>

**SUMMARY OF STATE LAWS REQUIRING NOTIFICATION OF A DATABASE SECURITY BREACH
(AS OF OCTOBER 1, 2008)**

STATE	LEGISLATION	SECTION	EFFECTIVE	SUMMARY
North Dakota	YES	N.D. Cent. Code §§ 51-30-01 et seq.	June 1, 2005	<p>Requires a person that conducts business in North Dakota and that owns or licenses computerized data that includes personal information disclose any security breach of the system to state resident whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person.</p> <p>Delayed notice permitted if consistent with law enforcement needs or measures necessary to determine scope of the breach and restore integrity of system.</p> <p>Substitute notice procedures permitted if cost exceeds \$250,000 or more than 500,000 persons are affected.</p> <p>Exempts financial institutions that are in compliance with the federal banking agencies' guidance issued on March 7, 2005.</p>
Ohio	YES	Ohio Rev. Code Ann. § 1349.19	February 17, 2006	<p>Requires that a person that owns or licenses computerized data that includes personal information disclose any security breach of the system to state residents whose unencrypted or unredacted personal information was or is reasonably believed to have been acquired by an unauthorized person, where there is a material risk of identity theft or other fraud to the resident.</p> <p>Delayed notice permitted if consistent with law enforcement needs or measures necessary to determine scope of the breach and restore integrity of the system.</p> <p>Substitute notice procedures permitted if cost exceeds \$250,000 or more than 500,000 persons are affected. Special provision for small businesses.</p> <p>Exempts financial institutions in compliance with federal law or regulatory requirements.</p> <p>If more than 1,000 persons must be notified, the person must notify the nationwide consumer reporting agencies of the timing, distribution and content of the notices.</p>

**SUMMARY OF STATE LAWS REQUIRING NOTIFICATION OF A DATABASE SECURITY BREACH
(AS OF OCTOBER 1, 2008)**

STATE	LEGISLATION	SECTION	EFFECTIVE	SUMMARY
Oklahoma	YES	Okla. Stat. tit. 24, §§ 161 et seq.	November 1, 2008	<p>Requires that any person that owns or licenses computerized data that includes personal information provide notice of any unauthorized access and acquisition of unencrypted and unredacted computerized data (or if encrypted, the breach involves a person with access to the encryption key) that compromises the security or confidentiality of personal information maintained by the person as part of a database of personal information regarding multiple individuals and that causes, or that the person reasonably believes has caused or will cause, identity theft or other fraud to any Oklahoma resident. Delayed notice permitted if consistent with law enforcement needs and measures necessary to determine the scope of the breach and restore the reasonable integrity of the system.</p> <p>Substitute notice procedures permitted if cost exceeds \$50,000 or more than 100,000 state residents are affected.</p> <p>Exempts financial institutions that are in compliance with the federal banking agencies' guidance issued on March 7, 2005 and other entities in compliance with requirements of its primary or functional federal regulator.</p>

SUMMARY OF STATE LAWS REQUIRING NOTIFICATION OF A DATABASE SECURITY BREACH

(AS OF OCTOBER 1, 2008)

STATE	LEGISLATION	SECTION	EFFECTIVE	SUMMARY
Oregon	YES	Ore. Rev. Stat. §§646A.602 et seq.	October 1, 2007	<p>Requires that a person that owns, maintains or otherwise possesses computerized data that includes a consumer's personal information provide notice to any Oregon resident of any unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of the resident's unencrypted personal information or encrypted personal information and key that was included in the information that was breached. Notice is not required if, after consultation with law enforcement agencies, the person determines there is no reasonable likelihood of harm to consumers.</p> <p>Delayed notice permitted if consistent with law enforcement needs and measures necessary to determine sufficient contact information for notices, scope of the breach and restore the reasonable integrity, security and confidentiality of the data.</p> <p>Substitute notice procedures permitted if cost exceeds \$250,000 or more than 350,000 persons are affected.</p> <p>Exempts persons in compliance with requirements of its primary or functional federal regulator, federal or state law, or the Gramm-Leach-Bliley Act as it existed as of October 1, 2007.</p> <p>If more than 1,000 persons must be notified, the person must notify the nationwide consumer reporting agencies of the timing, distribution and number of notices and police report number, if known.</p>

**SUMMARY OF STATE LAWS REQUIRING NOTIFICATION OF A DATABASE SECURITY BREACH
(AS OF OCTOBER 1, 2008)**

STATE	LEGISLATION	SECTION	EFFECTIVE	SUMMARY
Pennsylvania	YES	73 Pa. Cons. Stat. §§ 2301 et seq.	June 22, 2006	<p>Requires that an entity that maintains, stores or manages computerized data that includes personal information provide notice of any material breach of security of the system to state residents whose unencrypted and unredacted personal information was, or is reasonably believed to have been, accessed and acquired by an unauthorized person that causes or is reasonably believed to cause or will cause loss or injury to a resident.</p> <p>Delayed notice permitted if consistent with law enforcement needs or measures necessary to determine scope of the breach and restore integrity of system.</p> <p>Substitute notice procedures permitted if cost exceeds \$100,000 or more than 175,000 persons are affected.</p> <p>Exempts financial institutions in compliance with federal banking agencies' guidance issued on March 7, 2005, and other entities in compliance with requirements of its primary or functional federal regulator.</p> <p>If more than 1,000 persons must be notified, the person must notify the nationwide consumer reporting agencies of the timing, distribution and number of notices.</p>
Puerto Rico	YES	10 L.P.R.A. §§ 4051 et seq.	Law: January 19, 2006; Regulations: August 23, 2006	<p>Requires a person who owns or is custodian of a database for commercial use that includes a personal information archive disclose any unauthorized access to Puerto Rico citizens whose personal information was not protected with cryptographical codes beyond a password.</p> <p>Delayed notice permitted if consistent with law enforcement needs or measures necessary to restore the security of the system.</p> <p>Substitute notice permitted if cost exceeds \$100,000 or more than 100,000 persons are affected.</p> <p>Persons must notify the Dept. of Consumer Affairs within 10 days after a violation is detected. The Dept. will make a public announcement on the next working day if the person was unable to identify the affected individuals.</p>

**SUMMARY OF STATE LAWS REQUIRING NOTIFICATION OF A DATABASE SECURITY BREACH
(AS OF OCTOBER 1, 2008)**

STATE	LEGISLATION	SECTION	EFFECTIVE	SUMMARY
Rhode Island	YES	R.I. Gen. Laws §§ 11-49.2-1 et seq.	March 1, 2006	<p>Requires a person who conducts business in Rhode Island and that owns or licenses computerized data that includes personal information disclose any breach of security to state residents whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.</p> <p>No notice required if after an investigation and consultation with law enforcement the person determines there is no significant risk of identity theft.</p> <p>Delayed notice permitted if consistent with law enforcement needs or measures necessary to determine scope of the breach and restore integrity of system.</p> <p>Substitute notice procedures permitted if cost exceeds \$25,000 or more than 50,000 persons are affected.</p> <p>Exempts financial institutions that are in compliance with the federal banking agencies' guidance issued on March 7, 2005 or are subject to the GLBA.</p>
South Carolina	YES	S.C. Code Ann. §§ 39-1-90 et seq.	July 1, 2009	<p>Requires that a person conducting business in South Carolina that owns or licenses computerized data containing unencrypted or unredacted personal information notify state residents if that personal information was, or is reasonably believed to have been, acquired by an unauthorized person, 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 resident.</p> <p>Delayed notice permitted if consistent with law enforcement needs or measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.</p> <p>Substitute notice procedures permitted if cost exceeds \$250,000 or more than 500,000 persons are affected or insufficient contact information.</p> <p>Exempts financial institutions subject to the GLBA.</p> <p>If more than 1,000 persons must be notified, the person must notify the nationwide consumer reporting agencies and state Department</p>

**SUMMARY OF STATE LAWS REQUIRING NOTIFICATION OF A DATABASE SECURITY BREACH
(AS OF OCTOBER 1, 2008)**

STATE	LEGISLATION	SECTION	EFFECTIVE	SUMMARY
				of Consumer Affairs of the timing, distribution and content of the notices.
South Dakota	NO	--		
Tennessee	YES	Tenn. Code Ann. § 47-18-2107	July 1, 2005	Requires an “information holder” to disclose a breach of the security of the system to any Tennessee resident whose unencrypted computerized personal information was or is reasonably believed to have been acquired by an unauthorized person. “Information holder” is any person or business that conducts business in Tennessee and that owns or licenses computerized data that includes personal information. Delayed notice permitted if consistent with law enforcement needs or measures necessary to determine scope of the breach and restore integrity of system. Substitute notice procedures permitted if cost exceeds \$250,000 or more than 500,000 persons are affected. Exempts financial institutions subject to the GLBA. If more than 1,000 persons must be notified, the information holder must notify the nationwide consumer reporting agencies of the timing, distribution and content of the notices.
Texas	YES	Tex. Bus. & Com. Code Ann. §§ 48.001 et seq.	September 1, 2005	Requires a person that conducts business in Texas that owns or licenses computerized data that includes sensitive personal information disclose a breach of the security of the system to any state resident whose unencrypted sensitive personal information was or is reasonably believed to have been acquired by an unauthorized person. Delayed notice permitted if consistent with law enforcement needs or measures necessary to determine scope of the breach and restore integrity of system. Substitute notice procedures permitted if cost exceeds \$250,000 or more than 500,000 persons are affected.

**SUMMARY OF STATE LAWS REQUIRING NOTIFICATION OF A DATABASE SECURITY BREACH
(AS OF OCTOBER 1, 2008)**

STATE	LEGISLATION	SECTION	EFFECTIVE	SUMMARY
				If more than 10,000 persons must be notified, the person must notify the nationwide consumer reporting agencies of the timing, distribution and content of the notices.
Utah	YES	Utah Code Ann. §§ 13-44-101 et seq.	January 1, 2007	Requires a person that owns or licenses computerized data that includes personal information disclose a breach of the system security to any state resident after an investigation reveals that misuse of personal information for identity theft or fraud purposes has occurred or is reasonably likely to occur. Delayed notice permitted if consistent with law enforcement needs or measures necessary to determine the scope of the breach of system security and restore the integrity of the system. Exempts persons regulated by other federal or state law that give notice to Utah residents in accordance with the other applicable law.

SUMMARY OF STATE LAWS REQUIRING NOTIFICATION OF A DATABASE SECURITY BREACH

(AS OF OCTOBER 1, 2008)

STATE	LEGISLATION	SECTION	EFFECTIVE	SUMMARY
Vermont	YES	Vt. Stat. Ann. tit. 9, §§ 2430 et seq.	January 1, 2007	<p>Requires that any data collector that owns or licenses computerized personal information that includes personal information concerning a consumer must provide notice to affected consumers of the unauthorized acquisition of or access to computerized data that compromises the security, confidentiality or integrity of personal information maintained by the data collector. Notice need not be given if the data collector establishes that misuse is not reasonably possible and provides notice of that determination and an explanation to the State attorney general or department of banking, insurance, securities and health care administration, as applicable. Delayed notice permitted if consistent with needs of law enforcement or measures necessary to determine the scope of the breach and restore the reasonable integrity, security and confidentiality of the data system.</p> <p>“Data collector” is an entity that for any purpose, whether by automated collection or otherwise, handles, collects, disseminates, or otherwise deals with nonpublic personal information.</p> <p>Substitute notice via conspicuous website posting and notification to major statewide media can be given if cost of notice would exceed \$5,000, the class of affected persons to be provided written or telephonic notice exceeds 5,000, or the business does not have adequate information to provide notice as outlined above.</p> <p>If the affected class exceeds 1,000, the business must notify the nationwide consumer reporting agencies of the timing, distribution and content of the notice.</p> <p>Exempts financial institutions in compliance with the federal banking agencies’ guidance issued on March 7, 2005.</p>

**SUMMARY OF STATE LAWS REQUIRING NOTIFICATION OF A DATABASE SECURITY BREACH
(AS OF OCTOBER 1, 2008)**

STATE	LEGISLATION	SECTION	EFFECTIVE	SUMMARY
Virginia	YES	Va. Code Ann. § 18.2- 186.6	July 1, 2008	<p>Requires that a person that owns or licenses computerized data including personal information disclose a breach of the security of the system to the State Attorney General and any Virginia resident whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person and causes, or the person reasonably believes has caused or will cause, identity theft or another fraud.</p> <p>Delayed notice permitted if consistent with law enforcement needs or measures necessary to determine scope of the breach and restore integrity of system.</p> <p>Substitute notice procedures permitted if cost exceeds \$50,000 or more than 100,000 persons are affected or insufficient contact information.</p> <p>Notices must contain specified information.</p> <p>If 1,000 or more individuals must be notified, the entity must notify the nationwide consumer reporting agencies and State Attorney General of the timing, distribution and content of the notices.</p> <p>Entities subject to and in compliance with the GLBA or notification requirements of their primary or functional state or federal regulator are deemed in compliance.</p>

**SUMMARY OF STATE LAWS REQUIRING NOTIFICATION OF A DATABASE SECURITY BREACH
(AS OF OCTOBER 1, 2008)**

STATE	LEGISLATION	SECTION	EFFECTIVE	SUMMARY
Washington	YES	Wash. Rev. Code §19.255.010	July 24, 2005	<p>Requires a person that conducts business in Washington that owns or licenses computerized data that includes personal information disclose a security breach to any state resident whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person.</p> <p>Delayed notice permitted if consistent with law enforcement needs or measures necessary to determine scope of the breach and restore integrity of system.</p> <p>Notice of a technical breach is not required if it does not seem reasonably likely to subject customers to a risk of criminal activity. Substitute notice procedures permitted if cost exceeds \$250,000 or more than 500,000 persons are affected.</p>
West Virginia	YES	W. Va. Code Ann. §§ 46A-2A-101 et seq.	June 6, 2008	<p>Requires an individual or entity disclose a breach of the security of a computerized system to any resident 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 that the individual or entity reasonably believes has caused or will cause, identity theft or other fraud to any resident.</p> <p>Notice must be given if information is accessed or acquired in unencrypted form or person with access to encryption key is involved and it is reasonably believed that the breach has caused or will cause identity theft or fraud to a state resident. Notice must include information on how to place a fraud alert or security freeze.</p> <p>Delayed notice permitted if consistent with law enforcement needs or measures necessary to determine scope of the breach and restore integrity of system.</p> <p>Substitute notice procedures permitted if cost exceeds \$50,000 or more than 100,000 residents are affected.</p> <p>If 1,000 or more individuals must be notified, the entities other than those which must comply with Title V of the Gramm-Leach-Bliley Act must notify the nationwide consumer reporting agencies of the timing, distribution and content of the notices.</p>

**SUMMARY OF STATE LAWS REQUIRING NOTIFICATION OF A DATABASE SECURITY BREACH
(AS OF OCTOBER 1, 2008)**

STATE	LEGISLATION	SECTION	EFFECTIVE	SUMMARY
				Exempts financial institutions in compliance with the federal banking agencies' guidance issued on March 7, 2005.
Wisconsin	YES	Wis. Stat. § 895.507	March 31, 2006	<p>Requires an entity whose principal place of business is located in Wisconsin or an entity that maintains or licenses personal information in Wisconsin to make reasonable efforts to notify an individual (wherever located) within a reasonable time, not to exceed 45 days, if the individual's personal information has been acquired by an unauthorized person and there is material risk of identity theft or fraud to the subject. Notice must include certain specified information.</p> <p>An entity whose principal place of business is not located in Wisconsin must make reasonable efforts to notify each Wisconsin resident within a reasonable time, not to exceed 45 days, if the resident's personal information has been acquired by an unauthorized person and there is material risk of identity theft or fraud to the resident.</p> <p>Delayed notice permitted if consistent with law enforcement needs. If 1,000 or more individuals must be notified, the entity must notify the nationwide consumer reporting agencies of the timing, distribution and content of the notices.</p> <p>Exempts financial institutions subject to the GLBA that have a policy in effect concerning breaches of information security.</p>
Wyoming	YES	Wyo. Stat. §§ 40-12-501 et seq.	July 1, 2007	Requires that a person conducting business in Wyoming that owns or licenses computerized data including personal identifying information provide notice to a state resident of the unauthorized acquisition of unredacted, computerized data that materially compromises the security, confidentiality or integrity of the information and causes or is reasonably believed to cause loss or injury to a state resident. Notice is required if after a reasonable and prompt investigation the person determines the misuse of personal identifying information has occurred or is reasonably likely to occur.

**SUMMARY OF STATE LAWS REQUIRING NOTIFICATION OF A DATABASE SECURITY BREACH
(AS OF OCTOBER 1, 2008)**

STATE	LEGISLATION	SECTION	EFFECTIVE	SUMMARY
				<p>Delayed notice permitted if consistent with needs of law enforcement and measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. Substitute notice via conspicuous website posting and notification to major statewide media, including toll-free number, can be given if cost of notice would exceed \$10,000 for Wyoming based persons or businesses or \$250,000 for other non-Wyoming based businesses, the class of affected persons to be provided written or electronic notice exceeds 10,000 for Wyoming-based persons or businesses or 500,000 for non-Wyoming based businesses, or the person does not have sufficient contact information. Notice must include toll-free number an individual can use to contact the person collecting the data and learn the toll-free telephone numbers and addresses for the major credit reporting agencies. Exempts financial institutions in compliance with the federal banking agencies' information security guidelines.</p>

Copyright © 2008 by Schwartz and Ballen LLP. All rights reserved.