

State Privacy Law Summary

The table below contains a summary of state notification statutes, and exemptions to these statutes related to the unauthorized disclosure of customer non-public personal information. Forty-five states have enacted legislation requiring notification of security breaches. Alabama, Kentucky, Mississippi, New Mexico, and South Dakota do not have security breach laws enacted.

State	Brief Summary of Statutory Requirement	Exemption	Link to Statute
AL	N/A	N/A	N/A
AK	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, shall disclose a breach of security of an information system. 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.	Persons subject to the Gramm-Leach-Bliley Act (GLBA) are exempt from this requirement.	Sec. 45.48.010
AR	A person that conducts business in Arizona and owns or licenses unencrypted computerized data shall disclose after an investigation any incident of unauthorized acquisition and access to unencrypted or unredacted personal information to affected individuals. No notice is required if after an investigation the person determines that a breach has not occurred or is not reasonably likely to occur.	Persons subject to the privacy provisions of the GLBA or to the Health Insurance Portability and Accountability Act (HIPAA) are exempt. Arizona also provides that a person who complies with notification requirements or security breach procedures pursuant to the requirements of the person's primary or functional regulator is deemed in compliance with the state requirements.	Ark. Code Ann. §§ 4-110-101 through 108
AZ	A person that acquires, owns or licenses computerized data shall 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.	The Act does not apply to businesses regulated by state or federal law that provides greater protection to personal information and at least as thorough disclosure requirements for breaches of personal information as under Arkansas law.	Ariz. Rev. Stat. § 44-7501
CA	A person that conducts business in California and that owns, licenses or maintains computerized data shall 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. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.	A person that maintains notification procedures as part of an information security policy for the treatment of personal information is deemed to be in compliance with the notification requirements of the law if the person provides notification in accordance with that policy on breach of security and if the notification is consistent with the timing requirements of the law.	Cal. Civ. Code § 1798.29; Cal. Civ. Code § 1798.80-84
CO	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 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. 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.	A person that is regulated by state or federal law and that maintains procedures for a breach of security pursuant to the requirements of its primary or functional state or federal regulator is deemed to be in compliance with these requirements.	Col. Rev. Stat. § 6-1-716
CT	A person that owns, licenses or maintains computerized data shall 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. No notice required if after an investigation and consultation with law enforcement the person determines there is no reasonable likelihood of harm.	Any person that maintains a security breach procedure pursuant to the rules, regulations, procedures or guidelines established by their primary or functional regulator shall be deemed to be in compliance with the Connecticut law.	Conn. Gen. Stat. § 36a-701b
DE	A person that conducts business in the state and that owns or licenses computerized data shall 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. 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. 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.	An individual that is regulated by state or federal law and that maintains procedures for a breach of the security of the system pursuant to the laws, rules, regulations, guidance or guidelines established by its primary or functional regulator is in compliance with the act if the individual or commercial entity notifies affected residents in accordance with the maintained procedures.	Del. Code Ann. Tit. 6, §§ 12B-101 - 104
FL	A person that conducts business in Florida and that maintains computerized data in a system that includes personal information shall disclose a breach of the security of the system to any Florida resident whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. No notice required if after an investigation or consultation with law enforcement the person determines there is no reasonable likelihood of harm.	An entity that maintains notification procedures as part of an information security policy for the treatment of personal information, in which the notification is consistent with the timing requirements of the law or, pursuant to the rules, regulations, procedures or guidelines established by the entity's primary or functional federal regulator, is deemed to be in compliance with the notification requirements of the law.	Fla. Stat. ch. 817.5681
GA	Georgia 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. An "information broker" is a person or entity who collects information on individuals for the primary purpose of furnishing that information to third parties.	An "information broker" that maintains notification procedures as part of an information security policy is deemed to be in compliance with the notification requirements of the law if the information broker provides notification in accordance with the policy and consistent with the timing requirements of the law.	Ga. Code Ann. § 10-1-910 through 915

State	Brief Summary of Statutory Requirement	Exemption	Link to Statute
HI	Requires any business that owns, licenses, maintains or possesses personal information of Hawaii 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.	Financial institutions subject to the Interagency Guidelines and any health plan or healthcare provider that is subject to and in compliance with the privacy and security requirements of HIPAA are deemed compliant.	Haw. Rev. Stat. § 487N-1 through 487N-7
IA	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 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.	Entities with procedures that provide greater protection and notice, those required by other law to provide notice and those subject to GLB, are deemed compliant.	Iowa Code § 715C.1 et seq.
ID	An entity conducting business in the state that owns or licenses computerized data that includes personal information shall 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.	An entity that maintains notification procedures as part of an information security policy that are in compliance with state law is deemed compliant. An entity regulated by state or federal law that maintains procedures for a breach of security of the system pursuant to the requirements established by law or its primary or functional state or federal regulator is deemed in compliance with the Idaho law.	Idaho Code § 28-51-103 through 107
IL	A "data collector" that owns or licenses personal information shall disclose a breach of the security of the computerized system data to any Illinois resident whose unencrypted personal information is compromised. "Data collector" includes, but is 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.	A data collector that maintains notification procedures as part of an information security policy for the treatment of personal information is deemed to be in compliance with the notification requirements of the law if the data collector provides notification in accordance with that policy and if the notification is consistent with the timing requirements of the law.	815 Ill. Comp. Stat. 530/5-30
IN	Requires a data base owner to disclose a breach of the security of data 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.	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 (ex., Fair Credit Reporting Act or USA PATRIOT Act).	Ind. Code § 24-4.9
KS	A person that conducts business in the state that owns or licenses computerized data that includes personal information shall 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.	If an entity is regulated by state or federal law and maintains procedures for a breach of security pursuant to the requirements of its primary or functional regulator it is deemed to be in compliance.	Kan. Stat. Ann. §§ 50-7a01 through 7a04
KY	N/A	N/A	N/A
LA	A person that conducts business in the state or owns or licenses computerized data that includes personal information shall 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.	A financial institution that is subject to and in compliance with the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, issued on March 7, 2005, shall be deemed to be in compliance.	La. Rev. Stat. Ann. § 3071 through 3077
MA	Any person or agency that owns or licenses data that includes personal information shall 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 unencrypted 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.	Persons that maintain procedures for a breach of security pursuant to requirements of federal laws are exempt, 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.	Mass. Gen. Laws. ch. 93H, § 1 through 6
MD	Any person who maintains computerized data shall disclose after an investigation any breach of the security of the system involving unauthorized acquisition, release or use of an individual's computerized data 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 disclose after an investigation any breach of the security of the system involving unauthorized acquisition, release or use of an individual's computerized data to state residents whose unencrypted or unredacted personal information has been or it is reasonably possible will be misused.	Businesses that comply with the rules, regulations, procedures, or guidelines established by the primary or functional federal or State regulator of the business are deemed in compliance with this statute. Businesses that comply with the GLBA and other federal guidelines are also deemed in compliance.	Md. Code § 14-3501 through 3508
ME	Requires an "information broker" that maintains computerized data to disclose after an investigation any breach of the security of the system involving unauthorized acquisition, release or use of an individual's computerized data 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 disclose after an investigation any breach of the security of the system involving unauthorized acquisition, release or use of an individual's computerized data to state residents whose unencrypted or unredacted personal information has been or it is reasonably possible will be misused.	Persons that comply with security breach notification requirements of federal or State law, rules, regulations, procedures or guidelines are deemed to be in compliance under this law as long as the notification procedures are at least as protective as under this law.	Me. Rev. Stat. Ann. tit. 10, § 1346 through 1350-B
MI	A person that owns or licenses data that is included in a database shall disclose a breach of security to any Michigan resident whose unencrypted and unredacted personal information was accessed and acquired by an unauthorized person, or whose encrypted personal information was accessed and acquired by a person with unauthorized access to the encryption key, unless the person determines that the security breach has not or is not likely to cause substantial loss or injury or identity theft to one or more residents of Michigan.	Financial institutions subject to and in compliance with the federal banking agencies' guidance issued on March 7, 2005 or persons subject to and in compliance with HIPAA regulations regarding unauthorized access to customer information are deemed in compliance with the act.	Mich. Comp. Laws § 445.63 through 445.77
MN	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.	Exempts financial institutions as defined in Title V of the GLBA and entities subject to the privacy and security provisions of the HIPAA.	Minn. Stat. §§ 325E.61, 325E.64

State	Brief Summary of Statutory Requirement	Exemption	Link to Statute
MO	A person that owns or licenses personal information shall provide notice to state residents of a breach of security if after an investigation and consultation with law enforcement the person determines that a risk of identity theft or other fraud to any consumer is reasonably likely.	Financial institutions that comply with the federal banking agencies' guidance issued on March 29, 2005 or other persons in compliance with GLBA or requirements of their primary or functional federal or state regulators are deemed in compliance with this law.	Mo. Rev. Stat. § 407.1500 (2009 H.B. 62)
MS	N/A	N/A	N/A
MT	A person conducting business in Montana that owns or licenses computerized data including personal information shall disclose a breach of the security of the system to any Montana resident whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person.	A person that maintains notification procedures as part of an information security policy for the treatment of personal information is deemed to be in compliance with the notification requirements of the law if the person provides notification in accordance with that policy on breach of security and if the notification is consistent with the timing requirements of the law.	Mont. Code Ann. § 30-14-1704
NC	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) shall 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.	Financial institutions that are subject to and in compliance with the federal banking agencies' guidance issued on March 7, 2005 are deemed in compliance with the Act.	N.C. Gen. Stat. § 75-65
ND	A person conducting business in North Dakota that owns or licenses computerized data including personal information shall disclose a breach of the security of the system to any North Dakota resident whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person.	Exempts financial institutions that are in compliance with the federal banking agencies' guidance issued on March 7, 2005. A person that maintains notification procedures as part of an information security policy for the treatment of personal information is deemed to be in compliance.	N.D. Cent. Code §§ 51-30-01 through 07
NE	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.	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.	Neb. Rev. Stat. §§ 87-801 through 807
NH	A person doing business in New Hampshire who owns or licenses computerized data that includes personal information shall determine the likelihood that personal information has been or will be misused when it becomes aware of a security breach. If misuse has occurred or is reasonably likely to occur, or if a determination cannot be made, the person shall notify the affected individuals.	Any person which maintains procedures for security breach notification pursuant to state and federal laws shall be deemed to be in compliance with this subdivision if it acts in accordance with such laws.	N.H. Rev. Stat. Ann. §§ 359-C:19 through C:21
NJ	A business conducting 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.	A business that maintains notification procedures as part of an information security policy for the treatment of personal information is deemed to be in compliance with the notification requirements of the New Jersey law if the business provides notification in accordance with that policy on breach of security and if the notification is consistent with the requirements of the law.	N.J. Stat. Ann. §§ 56:8-161 through 166
NM	N/A	N/A	N/A
NV	A "data collector" that owns or licenses computerized data that includes personal information shall 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. A "data collector" includes any corporation, financial institution or other business entity that handles, collects, disseminates or otherwise deals with nonpublic personal information.	Data collectors subject to GLBA are exempt. A data collector that maintains notification procedures as part of an information security policy for the treatment of personal information is deemed to be in compliance with the notification requirements of the law if the data collector provides notification in accordance with that policy on breach of security and if the notification is consistent with the timing requirements of the law.	Nev. Rev. Stat. §§ 603A.010 through 603A.920
NY	A person conducting business in the state that owns or licenses computerized data shall 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.	N/A	N.Y. Gen. Bus. Law § 899-aa
OH	A person that owns or licenses computerized data that includes personal information shall disclose a breach of the security of the system which causes or reasonably is believed will cause a material risk of identity theft or other fraud to any Ohio resident whose unencrypted or unredacted personal information was, or is reasonably believed to have been, accessed or acquired by an unauthorized person.	Financial institutions that are required by and are in compliance with federal law or regulation to notify customers of an information security breach are exempt.	Ohio Rev. Code Ann. § 1349.19
OK	Any person that owns or licenses computerized data that includes personal information shall 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.	Financial institutions that comply with the federal banking agencies' guidance issued on March 7, 2005 or other entities in compliance with requirements of their primary or functional federal regulators are deemed in compliance with the act. Additionally, any entity that maintains notification procedures as part of an information privacy or security policy for the treatment of personal information that is consistent with the timing requirements of this act is deemed to be in compliance.	Okla. Stat. tit. 24, § 161, 2008 H.B. 2245
OR	Any person that owns, maintains or otherwise possesses computerized data that includes a consumer's personal information shall provide notice of any unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information maintained by a person to any Oregon resident whose personal information was included in the information that was breached, if after an appropriate investigation the person determines that no reasonable likelihood of harm to consumers has resulted or will result from the breach.	A person that complies with notification requirements or security breach procedures that provide greater protection to personal information and at least as thorough disclosure requirements pursuant to rules, regulations, procedures, guidance or guidelines established by that person's primary or functional federal regulator or a state or federal law is deemed in compliance. Additionally, any person that complies with GLBA is deemed in compliance.	Ore. Rev. Stat. §§ 646A.600 through 646A.628
PA	An entity that maintains, stores or manages computerized data that includes personal information shall provide notice of any breach of the security of the system to any Pennsylvania resident whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person. An entity also must provide notice of a breach if encrypted information is accessed and acquired in unencrypted form, if the security breach is linked to a breach of the security of the encryption or involves a person with access to the encryption key.	Financial institutions subject to and in compliance with the federal banking agencies' guidance issued on March 7, 2005 or other entities in compliance with the requirements of their primary or functional federal regulators are deemed in compliance. Additionally, any entity that maintains notification procedures as part of an information privacy or security policy for the treatment of personal information is deemed to be in compliance with the notification requirements of the law if the entity provides notification in accordance with its policies and if the notification is consistent with the timing requirements of the law.	73 Pa. Cons. Stat. §§ 2301 through 2329 (NO HYPERLINK)

State	Brief Summary of Statutory Requirement	Exemption	Link to Statute
RI	A person conducting business in the state that owns, licenses or maintains data in a system that includes personal information must disclose a breach of the security of the system which poses a significant risk of identity theft to any Rhode Island resident whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person.	A person that maintains notification procedures as part of an information security policy for the treatment of personal information in which the notification is consistent with the timing requirements of the law is deemed to be in compliance. Additionally, a financial institution that is in compliance with the federal banking agencies' guidance issued on March 7, 2005 or rules, regulations, procedures or guidelines established by the institution's functional regulator under the GLBA is deemed in compliance with the act.	R.I. Gen. Laws §§ 11-49.2-1 through 11-49.2-7
SC	A person conducting business in the state that owns or licenses computerized data containing personal information that is not rendered unusable through encryption, redaction or other means shall notify state residents if their 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.	A person that maintains notification procedures as part of an information security policy for the treatment of personal identifying information in which the notification is consistent with the timing requirements of the law is deemed to be in compliance. Additionally, a financial institution that is in compliance with the federal banking agencies' guidance issued on March 7, 2005 is deemed in compliance with the law. Banks or financial institutions subject to and in compliance with the GLBA privacy and security provisions are not subject to the law.	S.C. Code Ann. §§ 39-1-90 (NO HYPERLINK)
SD	N/A	N/A	N/A
TN	An "information holder" shall disclose a breach of the security of the system to any Tennessee resident whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. An "information holder" includes any person or business conducting business in Tennessee that owns or licenses computerized data that includes personal information.	Financial institutions subject to GLBA are exempt. An information holder that maintains notification procedures as part of an information security policy for the treatment of sensitive personal information is deemed to be in compliance with the notification requirements of the law if the information holder provides notification in accordance with that policy on breach of security and if the notification is consistent with the timing requirements of the law.	Tenn. Code Ann. § 47-18-2107
TX	A person conducting business in the state that owns or licenses computerized data that includes sensitive personal information shall disclose a breach of the security of the system that compromises the security, confidentiality or integrity of sensitive personal information, including data that is encrypted if the person accessing the data has the decryption key, to any Texas resident whose sensitive personal information was or is reasonably believed to have been acquired by an unauthorized person.	A person that maintains notification procedures as part of an information security policy for the treatment of sensitive personal information is deemed to be in compliance with the notification requirements of the law if the person provides notification in accordance with that policy on breach of security and if the notification is consistent with the timing requirements of the law.	Tex. Bus. & Com. Code Ann. § 521.001 et seq.
UT	A person who owns or licenses computerized data that includes personal information shall notify state residents if a reasonable and prompt investigation of a breach of system security reveals that the misuse of personal information for identity theft or fraud purposes has occurred, or is reasonably likely to occur.	Persons who are regulated by state or federal law and required to maintain security breach procedures are exempt if the person notifies affected Utah residents in accordance with the other applicable law.	Utah Code Ann. §§ 13-44-101 et seq.
VA	A person that owns or licenses computerized data including personal information shall 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.	A person that maintains notification procedures as part of an information privacy or security policy for the treatment of personal information consistent with the timing requirements of the law is deemed to be in compliance with the notification requirements of the law if the person provides notification in accordance with that policy. Persons subject to and in compliance with GLBA and persons that comply with the rules, regulations or guidelines of their primary or functional state or federal regulators are deemed in compliance with this law.	Va. Code Ann. § 18.2-186.6
VT	Any "data collector" that owns or licenses computerized personal information that includes personal information concerning a consumer shall provide notice of the unauthorized acquisition or access of 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 this determination and an explanation to the State Attorney General or the department of banking, insurance, securities and health care administration, as applicable.	A financial institution that is subject to the federal banking agencies' guidance issued on March 7, 2005 and National Credit Union Administration guidance issued on April 14, 2005 on unauthorized access to customer information are exempt from the law.	Vt. Stat. Ann. tit. 9, §§ 2430 et seq.
WA	A person conducting business in Washington that owns or licenses computerized data including personal information shall disclose a breach of the security of the system to any Washington resident whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. Notice of a technical breach of the security system is not required if it does not seem reasonably likely to subject customers to a risk of criminal activity.	A person that maintains notification procedures as part of an information security policy for the treatment of personal information is deemed to be in compliance with the notification requirements of the law if the person provides notification in accordance with that policy on breach of security and if the notification is consistent with the timing requirements of the law.	Wash. Rev. Code § 19.255.010
WI	An entity whose principal place of business is located in Wisconsin or an entity that maintains or licenses personal information in Wisconsin must make reasonable efforts to notify an individual (wherever located) if the entity knows the individual's personal information has been acquired by a person whom the entity has not authorized to acquire it and there is a material risk of identity theft or fraud to the subject.	The law specifically exempts entities subject to, and in compliance with the GLBA or persons with a contractual obligation to such an entity if the entity or person has in effect a policy concerning breaches of information security.	Wis. Stat. §§ 134.98 et seq.
WV	An individual or entity shall disclose a breach of the security of a computerized system to any West Virginia resident whose unencrypted or 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 of this state.	Financial institutions that respond to a breach in accordance with the federal banking agencies' guidance issued on March 7, 2005 are deemed in compliance. Entities that maintain their own notification procedures as part of an information privacy or security policy are deemed in compliance with the law if the entity provides notification in accordance with that policy and consistent with the timing requirements of this law. Entities that comply with the notification requirements or procedures pursuant to those established by the entity's primary or functional regulator also are deemed in compliance.	W. Va. Code Ann. §§ 46A-2A-101 et seq.
WY	An individual or commercial entity conducting business in the state that owns or licenses computerized data that includes personal identifying information shall provide notice to a state resident of the unauthorized acquisition of computerized data that is not redacted 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.	A financial institution that maintains notification procedures in accordance with the federal banking agencies' interagency guidelines for establishing information security standards are deemed in compliance with the law if the financial institution notifies Wyoming consumers in accordance with the federal guidelines.	Wyo. Stat. §§ 40-12-501 et seq.

Data Encryption

Below is are statutes from Massachusetts and Nevada related to data encryption.

State	Brief Summary of Statutory Requirement	Exemption	Link to Statute
State	Brief Summary of Statutory Requirement		Link to Statute
MA	All companies that own, license, store or maintain personal information concerning any Massachusetts resident must take comprehensive measures to protect that information from unauthorized access, disclosure or misuse. The new regulations impose a broad range of requirements, including obligation to encrypt all personal information of Massachusetts residents that is stored on any portable device (which includes laptops, flash drives, Blackberries or cell phones - to the extent feasible) that is transmitted over the Internet or by wireless connections. The effective date of the Rules has been changed to March 1, 2010.		201 CMR 17.00
NV	Nevada put into effect the nation's first data encryption law, effective October 1, 2008, which prohibits businesses from electronically transferring customers' personal data outside their organization unless it is encrypted (NRS 597.970). This law continues in effect until January 1, 2010. The law was amended and the effective date for the amended law is January 1, 2010. The amended law applies to a company doing business in Nevada that deals with nonpublic personal information, except for telecommunication providers and covers a company outside of Nevada that does business in Nevada. The definition of "personal information" is from the Nevada data breach law and means an individual's first name or first initial and last name in combination with their (i) Social Security Number (excluding the last four digits), (ii) driver's license number or identification card number or (iii) account number, credit card number or debit card number, together with any required security code permitting access to their financial account, when both the name and the foregoing data element are not encrypted. A company that does not accept a payment card (a credit card, charge card, debit card or similar card) in connection with a sale of goods or services must use encryption (i) to transfer any personal information through an electronic, nonvoice transmission (other than a facsimile) outside the company's secure system or (ii) when a data storage device (like a computer, cell phone, magnetic tape, electronic computer drive and optical computer drive) containing personal information is moved beyond the company's physical or logical controls. However, the amended law does not apply to data transmission over a secure, private communication channel for the (A) approval or processing of negotiable instruments, electronic fund transfers or similar payment methods or (B) issuance of reports regarding account closure due to fraud, substantial overdrafts, abuse of automatic teller machines or related information regarding a customer.		Nev. S.B. No. 227.