

# DISCLOSURE OF SECURITY BREACH

State	Code & Effective Date	Covered Entities	Penalties	Exemptions	Notification Requirements	Substitute Notice	Other Requirements
ARIZONA	§ 44-7501 December 31, 2006	Any person that conducts business in Arizona and owns or licenses computerized data which includes personal information of state residents.	Civil penalty not to exceed \$10,000 per security breach.	Entities governed by HIPAA and Gramm-Leach Bliley Act. If the information is redacted or secured by any other mean. Notification not required if person or a law enforcement agency determines that a security breach of system has not occurred.	Notice must be given to the victims of a security breach without unreasonable delay, unless disclosure impedes law enforcement investigation. Notice can be delivered in written, electronic or by telephone.	Substitute notice should be give by email or posting on website or notification in major state media if the cost exceeds \$50,000 or the affected class to be notified exceeds 100,000 persons, or does not have sufficient contact information.	If the entity or a law enforcement agency determine after investigation that breach does not compromise the security or confidentiality of personal information then notice is not required.
ARKANSAS	§ 4-110- 101 March 31, 2005	An Individual, business & state agency that obtain, own, or license personal information related to Arkansas residents.	Enforceable by the action of Attorney General.	Persons/business regulated by any state or Federal law that provides greater protection and lesser disclosure of personal information are exempt. If the data lost is in encrypted format.	Notice must be provided to the victims of a security breach without unreasonable delay, unless disclosure impedes law enforcement investigation. Notice can be delivered in written or electronic format or by telephonic.	Substitute notice should be given by email or posting on the website or notification in major state media if the cost exceeds \$250,000 or the affected class to be notified exceeds 500,000 persons, or does not have sufficient contact information.	Notice is not required if entity concludes that there is no reasonable likelihood of harm to consumers.
CALIFORNIA	§ 1798.82 July 1, 2003	A person / entity that operate or do business in California or any agency that owns or licenses computerized data which includes personal information. All agencies shall keep an accurate accounting of the date, nature, and purpose of each disclosure of a record.	Right of private action. A customer may recover a civil penalty not to exceeding \$3,000 per violation.	Business with less than 20 employees. If the data lost is in encrypted/redacted format.	Written or electronic notice must be given to the person within the most expedient time possible and without unreasonable delay.	Substitute notice can be given if the cost exceeds \$250,000, or the affected persons exceed 500,000, or the entity does not have contact information. Substitute notice can be delivered via Email, posting on web site or statewide media.	Notice not required if disclosure impedes a criminal investigation.

## DISCLOSURE OF SECURITY BREACH

State	Code & Effective Date	Covered Entities	Penalties	Exemptions	Notification Requirements	Substitute Notice	Other Requirements
<b>COLORADO</b>	§ 6-1-716 September 01, 2006	An individual or business entity that conducts operates in Colorado and owns or licenses computerized information which includes personal information of Colorado residents.	The Attorney General may take action in law or Equity to address violations.	Encrypted or redacted information or secured by any other method. Entities covered under Gramm-Leach-Bliley Act are exempt.	Notice must be provided within the most expedient time possible and without unreasonable delay, unless disclosure impedes law enforcement investigation. Notice can be in written or electronic format or by telephone.	Substitute notice can be given if the cost exceeds \$250,000, or the affected class of persons exceeds 500,000, or the entity does not have contact information. Substitute notice can consist of Email or by posting on web site or through statewide media.	Notice is not required if the entity determines after investigation that misuse of the data is not possible.
<b>CONNECTICUT</b>	§ 36a-701B January 01, 2006	Any person, who conducts business in Connecticut, and who, maintains computerized data which includes personal information.	Enforced by the Attorney General.	Any person or entity who maintains security breach procedures pursuant to the rules, regulations and procedures according to the Connecticut laws (§ 36a-701B) are exempt. Information secured by means of encryption or any other method.	Written, telephonic or electronic notice of security breach must be provided within the most expedient time possible and without unreasonable delay, unless disclosure impedes law enforcement investigation.	Substitute notice is allowed if the breach occurs on large scale.	Notice not required if the entity determines in consultation with the law enforcement agencies that there is no reasonable likelihood of harm to consumers.
<b>DELAWARE</b>	§ 12B-101-104 June 28, 2005	An individual or commercial entity that operates in Delaware and owns or licenses computerized information which includes personal information.	The Attorney General may bring an action in law or equity to address violations and for other relief that is appropriate to ensure proper compliance or to recover direct economic damages resulting from a violation.	Information lost is in encrypted format or if the entity or individual is regulated by another Federal or state law which requires breach notifications. Compliance with such notification requirements will be sufficient for the purpose of this statute.	Notice in writing or by electronic means must be provided to the victims within the most expedient possible time and without unreasonable delay, unless disclosure impedes law enforcement investigation. Written notification of breach must be provided to the Department of Justice.	Substitute notification can be given by email or posting on the web site or through statewide media if the cost of notice exceeds \$75,000, or that the affected class to be notified exceeds 100,000, or if the individual / commercial entity does not have sufficient contact information to provide notice.	If the entity concludes that the breach will not likely result in harms to the consumers.

## DISCLOSURE OF SECURITY BREACH

State	Code & Effective Date	Covered Entities	Penalties	Exemptions	Notification Requirements	Substitute Notice	Other Requirements
<b>FLORIDA</b>	§ 817.5681 July 1, 2005	Any person or entity that operates in Florida and maintains computerized data in a system that includes personal information.	If fails to notify within 45 days after the determination of breach is liable for fine not to exceed \$500,000. \$1,000 per day the breach goes undisclosed for up to 30 days, \$50,000 for each 30 day or thereof for up to 180 days. Administrative fine of up to \$500,000 If notification is not made within 180 days.	Encrypted Information.	Notice of security breach must be provided no later than 45 days following the determination of the breach in written or by electronic means unless disclosure impedes law enforcement investigation. If the notification is to be given to more than one thousand persons then the entity is required to inform all consumer reporting agencies without delay.	Substitute notice can be given if the cost exceeds \$250,000, or the affected persons exceed 500,000, or the entity does not have contact information. Substitute notice be given by Email or posting on web site or through statewide media.	Notification is not required if, after an investigation / consultation with relevant Federal, state, and local agencies reasonably determines that the breach will not likely result in harm to the individuals. Such determination must be documented and maintained for 5 years.
<b>GEORGIA</b>	§ 10-1-910 - 912 May 05, 2005	Any information broker (person or entity who maintains data for monetary fees or dues) which maintains computerized data which includes personal information.	---	Information if encrypted format or Redaction in any other manner.	Written or electronic notice of a security breach must be provided to affected citizens within the most expedient time possible and without unreasonable delay, unless disclosure impedes a criminal investigation.	Substitute notice by email, posting on website, or by notification in statewide media must be given in case of very large breaches. If the breach is for more than 10,000 individuals at one time, then the entity should also promptly notify all consumer reporting agencies.	---
<b>HAWAII</b>	§ 487 N-2 January 1, 2006	An agency, individual or commercial entities who conduct business in Hawaii state & owns or licenses computerized information which includes personal information or maintains such data of Hawaii residents.	The Attorney General or the executive director of consumer protection agency may bring an action. No such action may be brought against a government agency. Fine up to \$2,500 per violation.	Entities regulated by HIPAA are considered compliant & any other entities regulated by state or Federal laws that maintain procedures for addressing security breaches pursuant to those laws are exempt. Encrypted information.	Notice required if the personal information (lost incase of breach) is used illegally or is reasonably likely to occur or that creates a risk of harm to the person.	Substitute notice can be given if more than 200,000 people are affected, or the notice cost is \$100,000. Credit reporting agencies must be notified if more than 1,000 people are affected.	---

## DISCLOSURE OF SECURITY BREACH

State	Code & Effective Date	Covered Entities	Penalties	Exemptions	Notification Requirements	Substitute Notice	Other Requirements
IDAHAO	§ 28-51-105 July 1, 2006	An individual, agency or commercial entity that conducts business in Idaho and owns or licenses computerized information which includes personal information of Idaho resident.	Fine of \$25,000 per security breach.	Data maintained in encrypted format. An entity who comply with Federal or State security laws.	Notice must be provided to the Idaho resident, whose information is effected by security breach within the most expedient time possible and without unreasonable delay, unless disclosure impedes law enforcement investigation.	Substitute notice can be given via Email, posting the notice on the web site or via Statewide media in case of large security breach.	Notice not required if there is no material compromise on the security.
ILLINOIS	815 ILL. COMP. STAT. 530/10 January 1, 2006	An entity "data collector" that owns or licenses personal information of Illinois resident. Data collector can be government agencies, public and private universities, privately and publicly held corporations, financial institutions, retail operators, and any other entity that, for any purpose, handles, collects, disseminates, or otherwise deals with nonpublic personal information.	Violation of the statute constitutes an unlawful practice under the consumer fraud and deceptive business practices act.	Encrypted or redacted information by any means.	Notice in written or electronic format must be provided to the affected persons within the most expedient time possible and without an unreasonable delay.	Substitute notice by email, or notice in state wide media or posting on website can be given in case of large breaches.	---
INDIANA	§ 24-4.9 July 1, 2006	A Database owner who owns or licenses computerized information which includes personal information or a person who maintains computerized data but that is not a data base owner.	---	Information which is encrypted.	Written or electronic notice must be provided to affected persons within most expedient time and without unreasonable delay, unless disclosure impedes law enforcement investigation.	Substitute notice by email, notification by statewide media or by posting on website can be given. If more than 1,000 person needs to be notified, the state agency must also notify all consumer reporting agencies.	---

# DISCLOSURE OF SECURITY BREACH

State	Code & Effective Date	Covered Entities	Penalties	Exemptions	Notification Requirements	Substitute Notice	Other Requirements
KANSAS	§ 50-7a02 January 1, 2007	A person or business entity that conducts business in Kansas or a government subdivision or agency that owns or licenses computer based information which includes personal information.	Action against Insurance companies is brought before the insurance commissioner. Attorney General may also take actions to enforce.	Entities regulated by state or Federal regulations and entities who maintain safety procedures to avoid security breaches pursuant to this law are exempt. Information which is encrypted.	Written or electronic notice should be given to affected persons soon as possible and without unreasonable delay, unless disclosure impedes a criminal investigation. If more than 1,000 state residents need to be notified at one time then all consumer reporting agencies should also be informed.	Substitute notice by email, posting on website or notification via statewide media is allowed in case of large breaches.	Notification not required if the personal info which is lost or accessed by unauthorized individual is encrypted or redacted.
LOUISIANA	§ 3071 -3074 January 1, 2006	Any person or entity that conducts business in Louisiana or owns or licenses computerized data which includes personal information.	Fine can be imposed of \$1,000 per day for the first 30 days, and \$50,000 per day afterwards and maxim of \$500,000.	---	Written or electronic notice must be provided to affected persons as soon as possible without unreasonable delay, unless disclosure impedes law enforcement investigation.	Substitute notice can be given via email, posting on website or by notification in statewide media in case of large security breach.	Notice not required if after a reasonable investigation concludes that there is no reasonable likelihood of harm to the consumers.
MAINE	Tit. 10, § 1346 January 31, 2006	Businesses entities (private sector), information brokers and A 3rd-parties who maintain computerized data which contain personal information.	A fine of not more than \$500 per violation, up to a maximum of \$2,500 for each day.	Statute not applicable if the data lost is encrypted or redacted. Entities regulated by Gramm-Leach-Bliley Act.	Written/electronic notice must be provided to affected persons as expediently as possible and without unreasonable delay unless disclosure impedes law enforcement investigation.	Substitute notice by email, posting on websites and by notification in statewide media allowed only if the cost of providing notice exceeds \$5,000 or the affected personals exceeds by 1,000 or the does not have sufficient contact information.	If more than 1,000 persons need to be notified at one time then all consumer reporting agencies including appropriate state regulators agencies, Dept. of professional and financial regulation or the Attorney General. must also be notified.

## DISCLOSURE OF SECURITY BREACH

State	Code & Effective Date	Covered Entities	Penalties	Exemptions	Notification Requirements	Substitute Notice	Other Requirements
MARYLAND	Md. Code, § 14-3501 May 17, 2007	This law applies on Sole proprietors, Partnership, Corporation, Associations, or any other business entity, whether or not organized to operate (for profit making) who owns or licenses personal information or computerized data.	Fine of \$1000.00 for each violation. Subsequent violation: \$5000.00.	Entities will be deemed compliant with this law are the entities who are compliance with Gramm-Leach-Bliley Act and the entities who are in compliance with the requirements pursuant to the rules and regulations and procedures established by federal or state regulator.	Individual must be notified as early as possible if after investigation, it is determined that misuse of personal information is occurred or likely to be occurred. notification can be written, telephonic or by email.	Substitute notice can be given via E-mail, Posting the notice on Website, notification to statewide media. The Attorney General must be informed prior giving notice to residents. All consumers reporting agency should be informed if 1000 or more individuals needs to be notified.	Encrypted or redacted information or information protected by using another method which renders the information unreadable or unusable.
MASSACHUSETTS	H.B. 4144, Ch 93H August 2, 2007	A natural person, corporation, association, partnership, agency or any other legal entity.	The Attorney General may bring an action. A civil penalty of not more than \$5000 for each such violation and reasonable investigation costs, litigation & attorneys' fees.	Persons/business entities who act in accordance with the Federal laws, rules, regulation, guidance or guidelines relating to protection and privacy of personal information are deemed to be in compliance with this law.	A person or agency that maintain, stores, own or license or does not own or license data which include personal information shall provide notice to individuals without unreasonable delay and also notify the Attorney General & the director of the office of consumer affairs and business regulation of the breach.	Substitute notice via e-mail, posting notice on website, publication or broadcast through Media, if the cost exceeds \$250,000, or the affected residents exceeds 500,000 or the person or agency does not have sufficient contact information.	---
MICHIGAN	§ 445.71 June 29, 2007	State agencies, higher education institutes, individual, partnership, corporation, limited liability companies, association or other legal entities that own or licenses personal information.	Fine of \$250.00 for each violation and maximum is \$750,000.	Information if in Encrypted format. Financial institutions and entities regulated by HIPAA.	Notification required without unreasonable delay by email or telephone unless determined that breach has not likely to cause substantial loss to identity theft with respect state residents.	Substitute notice is allowed if the cost of providing notice exceed from \$250,000 or notice is to be provided to more than 500,000 residents.	---

# DISCLOSURE OF SECURITY BREACH

State	Code & Effective Date	Covered Entities	Penalties	Exemptions	Notification Requirements	Substitute Notice	Other Requirements
MINNESOTA	§ 325E.61 January 1, 2006	Any person, business or state agency doing business in Minnesota who owns or licenses computerized information which contains personal information.	---	Statute not applicable if the lost information is in encrypted format. Financial institutions and entities covered by HIPAA are exempt.	Written or electronic notice must be provided to the victims within the most expedient time possible and without unreasonable delay, unless disclosure impedes law enforcement investigation.	Substitute notice by email, posting of notification on web and by publication of notice in the statewide media is allowed in the case of very large breaches.	---
MONTANA	§ 30-14-1704 March 1, 2006	An entity, person or business that conducts business in Montana, and owns or licenses computerized data which includes personal information.	---	Information which is in encrypted format.	Written, electronic or telephonic notice must be provided to the victims without unreasonable delay, unless disclosure impedes law enforcement investigation. Notice required when the security breach is likely to occur harm or injury to a Montana resident.	Substitute notice by email, posting of notice on website and or by notification in statewide media is allowed in case of very large security breaches.	---
NEBRASKA	§ 87-803 July 13, 2006	Any commercial or Individual entity that conducts business in Nebraska and owns or licenses computerized data which includes personal information.	---	Information that is in Encrypted format or redacted by other means. Entities regulated by State or Federal law who maintain procedures for addressing security breaches.	Written, electronic or telephonic notice must be provided to victims of a security breach within the most expedient time possible and without unreasonable delay, unless disclosure impedes law enforcement investigation.	Substitute notice by email, notification in statewide media or by posting on website is allowed in the case of very large breaches.	Notification not required if the breach does not materially compromise the security, confidentiality or integrity of the personal information.

## DISCLOSURE OF SECURITY BREACH

State	Code & Effective Date	Covered Entities	Penalties	Exemptions	Notification Requirements	Substitute Notice	Other Requirements
NEVADA	§ 603A.220 October 1, 2005	An Entity which include government, businesses and associations, who handle, collect, disseminate or otherwise deal with non public personal information, or own or licenses computerized information.	Civil penalties enforceable by Attorney General.	Information kept in encrypted format. Entities governed by Entities governed by Federal and Gramm-Leach-Bliley Act.	Notice should be provided to the victims without unreasonable delay and must also notify credit reporting agencies if more than 1,000 people are affected.	Substitute notice by email, notification in statewide media or by posting on website is allowed in the case of very large breaches.	---
NEW HAMPSHIRE	§ 359-C:19-21 January 1, 2007	Any person or entity that conducts business in New Hampshire and owns or licenses computerized data which includes personal information of NH resident.	Fine \$10,000 per violation.	State or Federal regulated entities that address the security issue pursuant to this law.	Written, electronic or telephonic notice must be provided to affected persons of a security breach within the most expedient time possible and without unreasonable delay.	Substitute notice by email, notification in statewide media or by posting on website is allowed in the case if the cost of providing notice exceeds \$5,000 or the individuals to be notified exceeds 1000.	---
NEW JERSEY	§ 56:8-163 January 01, 2006	A business entity that conducts business in NJ or any public entity that compiles or maintain computerized data which include personal information and any business or public entity that compiles or maintain computerized record that includes personal information on behalf of another business or public entity.	---	Personal information if secured by encryption or by any other method or technology that renders the personal information unreadable or unusable.	Written/ electronic notice must be provided to the victim of a security breach within the most expedient time possible & without unreasonable delay unless disclosure impedes law enforcement investigation. An entity must report the breach of security to the Division of State Police prior to informing the victims.	Substitute notice if the cost of providing notice exceeds \$250,000, or the affected class to be notified exceeds 500,000, can be given via email, posting the notice on the web site or via statewide media. If more than 1,000 persons need to be notified at one time of a security breach then consumer reporting agencies should also be informed.	Disclosure of a Security breach not required to a customer if the business or public entity establishes that misuse of the information is not reasonably possible. Such determinations must be documented in writing and retained for five (5) years.

# DISCLOSURE OF SECURITY BREACH

State	Code & Effective Date	Covered Entities	Penalties	Exemptions	Notification Requirements	Substitute Notice	Other Requirements
NEW YORK	§ 899-aa December 8, 2005	An entity that owns or licenses computerized information that includes private information and any person or business entity that conducts business in New York which owns or licenses computerized data containing private information.	Civil penalty of \$5,000 or up to \$10,000 per instance if failed to notify, the latter amount shall not exceed \$150,000.	Statute not applicable if the personal data that was lost is in encrypted format.	Written or electronic notice to the victims must be provided within the most expedient time possible and without unreasonable delay, unless disclosure impedes law enforcement investigation. If more than 5,000 persons at one time need to be informed, all consumer reporting agencies must also be notified.	Substitute notice by email, statewide media or by posting on website is allowed in case of very large breaches. Attorney General, and the Office of Cyber Security and Critical Infrastructure Coordination must also be notified.	---
NORTH CAROLINA	§ 75-65 December 1, 2005	A business that owns or licenses personal information of residents of North Carolina or any business that conducts business in North Carolina who owns or licenses personal information in any form, whether computerized, paper, or in any other manner.	Civil penalties.	Information if encrypted or Redacted in any other means which renders this in unreadable format.	Victims should be informed within the most expedient time possible and without unreasonable delay, unless disclosure impedes law enforcement investigation. Written, electronic or telephonic notice can be provided. If more than 1,000 persons need to be notified at one time then all consumer reporting agencies should also be informed.	Substitute notice by means of email, state wide media or by posting on website can be given if the cost of providing notices exceed \$250,000 or that the affected class to be notified exceeds 500,000.	Notice not required if the entity concludes that security breach is not likely to cause or create a material risk of harm to state residents.

# DISCLOSURE OF SECURITY BREACH

State	Code & Effective Date	Covered Entities	Penalties	Exemptions	Notification Requirements	Substitute Notice	Other Requirements
NORTH DAKOTA	§ 51-30-01 June 1, 2005	A person that conducts business in North Dakota and owns or licenses computerized data which includes personal information of State residents.	The Attorney General may take action.	Information is encrypted or secured by any other method or technology that renders the personal information unreadable or unusable. Federally regulated institutions are exempt.	Written or electronic notice must be provided to the victims within the most expedient time possible and without unreasonable delay, unless disclosure impedes law enforcement investigation.	Substitute notice by email, posting of notice on website or by notification in state media is allowed in the case of very large breaches.	---
OHIO	§ 1349.19 February 17, 2006	Any state agency or agency of a political subdivision or any person that owns or licenses computerized data which includes personal information.	Civil penalty of up to \$1,000 for every day of noncompliance and up to \$5,000 per day after 60 days, and up to \$10,000 per day after 90 days.	Information encrypted or redacted by using any other means. Entities in compliance & regulated by Federal regulations, Social Security Act, and HIPAA are exempt.	Written and electronic notification must be provided to a victims no latter than 45 days following the discovery of the breach, unless disclosure impedes law enforcement investigation. If more than 1,000 persons need to be notified at one time then also promptly notify all consumer reporting agencies.	Substitute notice by email, posting on web or by printing in statewide media allowed for businesses with less than ten 10 employees when notification costs exceed \$10,000.	Notification not required in case breaches did not cause material risk of identity theft or other fraud to an Ohio resident
OKLAHOMA	74 OKLA. § 3113.1 June 8, 2006	Any state agency, state board, commission or other unit or subdivision of state government that owns or licenses computerized information which includes personal information or maintains personal information of resident of Oklahoma.	---	Encrypted Information.	Written or electronic notice should be given in case of a security breach/loss of personal information in the most expedient time possible & without unreasonable delay. The notification may be delayed if law enforcement agency determines that notification will impede a criminal investigation.	Substitute notice can be given in case persons to be notified are 500,000 or the cost is \$250,000.00, by email, posting of the notice on the agency's web site or notification to major statewide media.	---

# DISCLOSURE OF SECURITY BREACH

State	Code & Effective Date	Covered Entities	Penalties	Exemptions	Notification Requirements	Substitute Notice	Other Requirements
OREGON	Ch. 759 S.B. 583 October 1, 2007	Any person who owns, maintains or possess computerized data which includes personal information shall provide notice of any unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of an individuals personal information.	In addition to the civil penalties in accordance with OCR 183.745 for every violation a penalty of not more than \$1,000 payable to the general fund of the state treasury and for in case of a continuing violation, each day's continuance is a separate violation, but the maximum penalty for any occurrence shall not exceed \$500,000.	Entities who comply with the Gramm-Leach-Bliley Act and who are in compliance with the notification requirement imposed by their primary or functional Federal regulator or by another state or Federal law.	Written, electronic or telephone notice must be provided in the most expeditious time possible without unreasonable delay. If the number of individuals whose personal information is compromised exceeds 1,000 at one time, All nationwide consumer reporting agencies must also be notified.	Substitute notice may be provided through posting of the notice on website and notification to major statewide television and newspaper media if the number of affected person is 350,000 or the cost of notification exceeds \$250,000.	Notice not required if, after investigation/consultation with federal, state or local agencies, the person determines that no likelihood of harm to the consumers has resulted or will result from the breach. Such determination must be documented and kept for 5 years.
PENNSYLVANIA	§ 2302 June 2006	An entity: individual, business or a state agency that maintains, stores, or manages computerized information containing personal information.	Violation of this act shall be deemed to be an unfair or deceptive act or practice in violation of trade practices and consumer protection law. The Attorney General shall have exclusive authority to bring an action.	If the information is in encrypted or redacted format. Entities in compliance with the Federal regulations are exempt.	Notice must be provided to the effected personals within the most expedient time possible and without unreasonable delay, unless disclosure impedes law enforcement investigation. Notice can be given via telephonic, written or via email.	Substitute notice by email, posting on website or by notification is statewide media can be given in the case of large security breaches. If more than 1,000 persons need to be notified at one time then all consumer reporting agencies must also be notified.	Notice is not required to be given if responsible entity concludes that the breach did not harm the personal information.
RHODE ISLAND	§ 11- 49.2-1 March 1, 2006	Any person or business entity that conducts business in Rhode Island and that owns or licenses computerized information which contains personal information.	A penalty of not more than a hundred dollars (\$100) per occurrence & not more than twenty-five thousand dollars (\$25,000) may be adjudged against a defendant.	Encrypted Information, HIPAA covered entities.	Written or electronic notice to be provided to the effected person incase of security breach, within the most expedient time possible and without unreasonable delay unless disclosure impedes law enforcement investigation.	Substitute notice by email, posting of notice on web or by a notification is statewide media must be given when the number of affected persons exceeds 50,000 and notification costs exceed \$25,000.	Notice not required if law enforcement agencies after an appropriate investigation conclude that there is no significant risk of identity theft.

# DISCLOSURE OF SECURITY BREACH

State	Code & Effective Date	Covered Entities	Penalties	Exemptions	Notification Requirements	Substitute Notice	Other Requirements
TENNESSEE	§ 47-18-2107 July 1, 2005	A person or business entity that conducts business or any agency of Tennessee or political subdivisions, that own or licenses computerized information which includes personal information.	Civil penalty of whichever of the following is greater: \$10,000, \$5,000 per day for each day that a person's identity has been assumed or ten 10 times the amount obtained or attempted to be obtained by the person using the identity theft. This civil penalty is supplemental, cumulative and in addition to any other penalties and relief available under the Tennessee Consumer Protection Act. Any violation of terms or order issued pursuant to this by the Attorney general, a civil penalty of not more than \$5,000 for each and every violation.	Information if in encrypted format, the provisions of this section shall not apply to any person who is subject to the provisions of Title V of the Gramm-Leach-Bliley Act.	Notice must be provided to the person whose information is lost because of security breach, within the most expedient time possible and without unreasonable delay unless disclosure impedes law enforcement investigation.	Substitute notice can be given by email, posting of the notice on website, notification to major statewide media in case of very large breaches.	If the personal information that was lost or accessed by an unauthorized individual is encrypted then notice is not required.
TEXAS	§ 48.103 September 1, 2005	Any person that conducts business in Texas and owns or licenses computerized information which contains sensitive personal information. Any person that maintain computerized sensitive personal information of Texas citizens but does not own that information.	Civil penalty of at least \$2,000 but not more than \$50,000 for each violation.	Information in encrypted format.	Written / electronic notice must be provided to person whose information is lost in a result of security breach, within the most expedient time possible and without unreasonable delay unless disclosure impedes law enforcement investigation.	Substitute notice by email, posting on website or printing in state wide media is allowed in the case of very large breaches. If the incident occurred and the persons to be notified are more than 10,000 at one time, it should be promptly notified to all consumer reporting agencies.	Notice not required if the personal data which is lost or accessed by an unauthorized individual is encrypted.

# DISCLOSURE OF SECURITY BREACH

State	Code & Effective Date	Covered Entities	Penalties	Exemptions	Notification Requirements	Substitute Notice	Other Requirements
UTAH	§ 13-44-202 January 1, 2007	A person who owns or licenses computerized data that includes personal information related to Utah resident.	Penalty not greater than \$2,500 per violation or series of violations concerning a specific consumer, and not more than \$100,000 in the aggregate for related violations concerning more than one consumer.	Encrypted information or protected by another method that the data is unreadable or unusable. An entity regulated by state or Federal law that maintains procedures for addressing security breaches pursuant to those laws are exempt.	Notice must be provided to the effected residents of Utah within the most expedient time possible and without unreasonable delay. Notice can be delayed if impedes by law enforcement agencies. Notice can be sent by paper, electronically or by telephone.	Notice of the security breach can be provided via publication in a newspaper in case of large data loss.	---
VERMONT	§2435 January 01, 2007	State agencies, political subdivisions, public/private universities, private/public corporations, limited liability companies, financial institutions, retail operators, & any other entity that, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates, or deals with nonpublic personal information.	---	Excludes information redacted or protected by another method that renders the data unreadable or unusable. Encrypted information.	Any data collector that owns or licenses computerized personal information or a data collector who maintains or possesses computerized data containing personal information concerning a consumer shall notify of the breach in the most expedient time possible and without unreasonable delay.	Substitute notice allowed when cost of providing notice exceeds \$50,000 or affected individuals to be notified exceeds 5,000. If more than 1,000 persons must be notified at one time, CRA must also be notified or if exceeds 5,000 persons.	Security breach notice not required if the data collector establishes that misuse of information is not possible and provides notice. They shall provide notice of its determination and detailed explanation to Attorney General or to dept. of banking, insurance, securities, and health care administration.
WASHINGTON	Tit. 19 § 255.010 July 24, 2005	Any person or business entity which conducts business and owns or licenses computerized data which includes personal information or any person/business who maintains or licenses computerized data which includes personal information but do not own it.	Any customer injured by a violation of this section may institute a civil action to recover damages	---	Notice must be provided to the effected person by security breach, within the most expedient time possible and without unreasonable delay unless disclosure impedes law enforcement investigation. The notice can be in written or electronic.	Substitute notice allowed in the case of very large breaches by e-mail, posting the notice on the web site, notification via major statewide media.	Notice not required in case of a breach of the security system which does not reasonably affect consumers to a criminal offense.

# DISCLOSURE OF SECURITY BREACH

State	Code & Effective Date	Covered Entities	Penalties	Exemptions	Notification Requirements	Substitute Notice	Other Requirements
WISCONSIN	§ 895.507 March 31, 2006	Any entity (including State and local governments) that conduct business in Wisconsin and deals with personal information, maintain or maintains a depository account for a Wisconsin resident or lends money to a Wisconsin resident.	---	Entities in compliance with already established Federal & State privacy regulations. HIPAA covered Entities. Gramm-Leach-Bliley Act covered entities are excluded. Information if in encrypted format.	Written/electronic notice must be provided within reasonable time period within 45 days, unless disclosure impedes law enforcement agency. If in a single incident 1000 persons data is affected, all consumer reporting agencies must be informed.	---	Notice is not required if the breach does not create “a material risk of identity theft or fraud,” or if the personal information was obtained in good faith and is used for a lawful purpose.
WYOMING	§ 40-12-501 July 1, 2006	Any individual or commercial entity who conducts business in the State of Wyoming and owns or licenses, or maintains computerized data which includes personal information.	The Attorney General may bring an action in law or equity to address any violation and for other relief that may be appropriate to ensure proper compliance, to recover damages, or both. This penalty shall not have any effect upon any other recourse available to the affected individual.	---	Wyoming law requires that written or electronic notice must be given in the most expedient time possible to a state resident of the unauthorized acquisition of computerized data which causes or is reasonably believed to cause loss or injury.	Substitute notice via posting on website & notification in statewide media if notice cost exceed \$10,000 for Wyoming based entity & \$250,000 for other entities, or affected individuals exceeds 10,000 for Wyoming based entity, & 500,000 for other entities or if don't have enough contact information.	If after a reasonable and prompt investigation of a breach of the security the entity determines that the personal information will not be misused.
District of Columbia	§ 28-3851 July 1, 2007	A person or entity doing business in the district that owns or licenses computerized data that includes personal information disclose the unauthorized acquisition of computerized or other electronic data, or any equipment or device storing such data.	Civil penalty not exceeding \$100 for each violation, costs of the action, & the attorney’s fee. Violation may institute action to recover actual damages, costs of action, & attorney’s fees. Attorney General may enforce by seeking temporary or permanent injunctive relief, damages.	A person or entity that maintains notification procedures as part of an information security policy or consistent with the timing requirements of the law or pursuant to the Gramm-Leach-Bliley Act, is deemed to be in compliance with the notification requirements of the law.	Written or electronic notice must be made in the most expedient time possible, without unreasonable delay, and consistent with the needs of law enforcement.	Substitute notice via E-mail, posting on the business’s website & notification to major media, can be given if the cost of providing notice would exceed \$50,000, there are more than 100,000 affected individuals, or the person or business does not have sufficient contact information.	---