MINTZ LEVIN

STATE DATA SECURITY BREACH NOTIFICATION LAWS

Please note: This chart is for informational purposes only and does not constitute legal advice or opinions regarding any specific facts. You should seek the advice of competent legal counsel when reviewing options and obligations in responding to a particular data security breach. Laws and regulations change quickly in the data security arena. This chart is current as of October 1, 2011.

The general definition of "personal information" or "PI" used in the majority of statutes is: An individual's first name or first initial and last name plus one or more of following data elements: (i) Social Security number, (ii) driver's license number or state-issued ID card number, (iii) account number, credit card number or debit card number combined with any security code, access code, PIN or password needed to access an account and generally applies to computerized data that includes PI. When a statute varies from that definition, it will be pointed out in the chart.

As of October 1, 2011, Alabama, Kentucky, New Mexico and South Dakota do not have any laws related to security breach notification.

This chart provides general information and not legal advice regarding any specific facts or circumstances. For more information about security breach notification laws, or other data security matters, please contact the Mintz Levin attorney with whom you work, or Cynthia Larose (cjlarose@mintz.com / 617.348.1732), Dianne Bourque (dbourque@mintz.com / 617.348.1614), Stephen Bentfield (sbentfield@mintz.com / 202.585.3515) or Stu Eaton (seaton@mintz.com / 650.251.7726).

State and Bill Number	Data and consumers protected/Definition of Breach	Covered entities	Notice Procedures/ Timing/Exemptions	Encryption Safe Harbor	General & Preemption	Other provisions	Penalties	Private Cause of Action

MINTZ LEVIN

State and Bill Number	Data and consumers protected/Definition of Breach	Covered entities	Notice Procedures/ Timing/Exemptions	Encryption Safe Harbor	General & Preemption	Other provisions	Penalties	Private Cause of Action
Alaska H.B. 65 Effective 7/09 Alaska Stat. Tit. 45. Ch. 48. §§ 10 to 90	Personal information of Alaska residents, including a separate data element for passwords, PINs or other access codes for financial accounts. Applies to data in both electronic and paper formats. Security Breach Definition: An unauthorized acquisition or reasonable belief of unauthorized acquisition of personal information that compromises the security, confidentiality or integrity of the personal information maintained.	Any person doing business, any person with more than 10 employees, and any state or local governmental agency. Judicial branch agencies are not covered.	Written or electronic notice must be provided to victims of a security breach in the most expeditious time possible and without unreasonable delay, unless disclosure impedes a criminal investigation. Substitute notice by means prescribed in the statute allowed in the case of very large breaches. If an entity is required to notify more than 1,000 state residents of a breach, it must also notify without unreasonable delay all consumer credit reporting agencies that compile and maintain files on consumers on a nationwide basis. Notice not required if, after an investigation and written notice to the attorney general, the entity determines that there is not a reasonable likelihood that harm to the consumers will result. The determination must be documented in writing and maintained for five years. Exemption for good-faith acquisition by an employee, so long as PI not used for an illegitimate purpose or make further unauthorized disclosure. **No likelihood of harm PLUS written notification to AG.**	Statute not applicable if the personal data that was lost, stolen, or accessed by an unauthorized individual is encrypted or redacted.	Entities subject to Title V of the Gramm Leach Bliley Act of 1999, 15 U.S.C. § 6801, et seq ("GLBA") are exempt.	A waiver of the statute is void and unenforceable. Authorizes a state agency to promulgate implementing regulations at any point after July 1, 2009.	Governmental agencies are liable to the state for a civil penalty of up to $500 for each state resident who was not notified, but the total civil penalty may not exceed $50,000. The Department of Administration may enforce violations by governmental entities. Entities that are not governmental agencies are subject to state fair trade laws under AS 45.50.471 - 45.50.561. Entities are liable for civil penalties up to $500 per resident, with the total civil penalty not exceeding $50,000. Damages awarded under AS 45.50.531 are limited to actual economic damages that do not exceed $500, and damages awarded under AS 45.50.537 are limited to actual economic damages.	Yes. A person injured by a breach may bring an action against a non-governmental entity. Private actions may not be brought against governmental agencies.

MINTZ LEVIN

State and Bill Number	Data and consumers protected/Definition of Breach	Covered entities	Notice Procedures/ Timing/Exemptions	Encryption Safe Harbor	General & Preemption	Other provisions	Penalties	Private Cause of Action
Arizona S.B. 1338 Ariz. Rev. Stat. Tit. 44, Ch. 32, 44-7501	Personal information of Arizona residents **Security Breach Definition:** An unauthorized acquisition of unencrypted or unredacted computerized data that materially compromises the security or confidentiality of PI maintained by a covered entity as part of a data base of PI regarding multiple individuals and that causes or is reasonably likely to cause substantial economic loss to an individual.	Any person that conducts business in Arizona and owns or licenses unencrypted computerized data that includes personal information.	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 means prescribed in the statute allowed in the case of larger breaches. Notice not required if the breached entity or a law enforcement agency determine after a reasonable investigation that the breach does not materially compromise the security or confidentiality of personal information. Exemption for good-faith acquisition by an employee or agent, so long as PI not used for a purpose unrelated to the covered entity or subject to further willful unauthorized disclosure.	Statute not applicable if the personal data that was lost, stolen, or accessed by an unauthorized individual is encrypted or redacted. "Encrypted" defined as "an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without use of a confidential process or key." "Redact" defined as altering or truncating data "such that no more than the last four digits of a social security number, driver license number, nonoperating identification license number, financial account number or credit or debit card number is accessible as part of the personal information."	Entities that comply with the notification requirements or security breach procedures pursuant to the rules, regulations, procedures, guidance or guidelines established by the entities' primary or functional federal regulator are exempt. Entities subject to Title V of the GLBA as well as entities covered by the Health Insurance Portability and Accountability Act ("HIPAA") are exempt.	Third-party data notification: if covered entity maintains unencrypted data that includes PI that covered entity does not own, covered entity shall notify and cooperate with the owner or licensee of the information of any breach following discovery of the breach without unreasonable delay. "Cooperation" shall include sharing information relevant to the breach with the owner or licensee. The owner or licensee of the data shall provide notice to the individual, unless any agreement between the covered entity and the owner or licensee provides otherwise.	Actual damages for a willful and knowing violation of the statute. Civil penalty not to exceed $10,000 per breach of the security of the system or series of breaches of a similar nature that are discovered in a single investigation.	No. Enforcement by Attorney General only.

MINTZ LEVIN

State and Bill Number	Data and consumers protected/Definition of Breach	Covered entities	Notice Procedures/ Timing/Exemptions	Encryption Safe Harbor	General & Preemption	Other provisions	Penalties	Private Cause of Action
Arkansas S.B. 1167 Ark. Code tit. 4, ch. 110, §§ 101 to 108	Personal information of Arkansas residents. Personal information defined as the first name or initial and last name of an individual, with one or more of the following data elements: social security number, driver's license or state identification card number, credit card or debit card number, or a financial account number with any code that would provide access to the account ("personal information"). **Definition of "personal information" includes medical data**.	Individuals, businesses, and state agencies that acquire, own, or license personal information about Arkansas residents.	Written or electronic 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 means prescribed in the statute allowed in the case of very large breaches. Notice not required if the entity responsible for the data concludes that there is no reasonable likelihood of harm to consumers.	Statute not applicable if the personal data that was lost, stolen, or accessed by an unauthorized individual is encrypted.	Entities regulated by any state or federal law that provides greater protection to personal information and similar disclosure requirements are exempt. Any covered entity that maintains and proceeds in compliance with its own notification procedures as part of an information security policy for treatment of PI and is otherwise consistent with timing requirements of statute is deemed to be in compliance.	Covered entities must implement and maintain reasonable security procedures and practices to protect the personal information. Data destruction or encryption mandatory when personal information records are discarded. Third party notification – Covered entity must notify owner or licensee of data that includes PI of any breach of security immediately following discovery	Fines consistent with state fair trade laws.	No.

MINTZ LEVIN

State and Bill Number	Data and consumers protected/Definition of Breach	Covered entities	Notice Procedures/ Timing/Exemptions	Encryption Safe Harbor	General & Preemption	Other provisions	Penalties	Private Cause of Action
California S.B. 1386 Cal. Civ. Code §§ 56.06, 1785.11.2, 1798.29, 1798.82 Amended by A.B. 1298 SB 24 effective **January 1, 2012**	Personal information of California residents – **Amendment expands the scope of covered information to include medical information and health insurance information.** Security Breach; An unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of PI maintained by a covered entity.	Any person or business that conducts business in California or any state agency that owns or licenses computerized data that includes personal information. NOTE: provisions governing maintenance of PI not owned by the covered entity appear applicable to any entity maintaining information on CA residents, whether or not the entity conducts business in CA.	Written or electronic notice must be provided to victims of a security breach within the most expedient time possible and without unreasonable delay, unless disclosure impedes a criminal investigation. Substitute notice by means prescribed in the statute allowed in the case of very large breaches. Any covered entity that maintains and proceeds in compliance with its own notification procedures as part of an information security policy for treatment of PI and is otherwise consistent with timing requirements of statute is deemed to be in compliance. Exemption for good-faith acquisition by an employee or agent, so long as PI not used or subject to further willful unauthorized disclosure. 1/1/2012: Requires specific notice content, including a general description of the incident, the type of information breached, the time of the breach and toll-free numbers and addresses of the major credit card reporting agencies in CA. Requires notice to CA Attorney General if a single breach affects more than 500 Californians.	Statute not applicable if the personal data that was lost, stolen, or accessed by an unauthorized individual is encrypted.	Compliance cannot be waived by the affected individual	Entity responsible for data required to take all reasonable steps to destroy a customer's records that contain personal information when the entity will no longer retain those records. Third party notification: If a covered entity maintains computerized data that includes PI that the entity does not own, the entity must notify the owner or licensee of the information of any breach of security immediately following discovery.	Civil remedies available for violation of the statute.	Yes.

State and Bill Number	Data and consumers protected/Definition of Breach	Covered entities	Notice Procedures/ Timing/Exemptions	Encryption Safe Harbor	General & Preemption	Other provisions	Penalties	Private Cause of Action
Colorado H.B. 1119 Col. Rev. Stat. tit. 6, art. 1, §6-1-716	Personal information of Colorado residents. Security Breach: An unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of the PI.	Individual or commercial entity that conducts business in Colorado and owns or licenses computerized data that includes personal information.	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 means prescribed in the statute allowed in the case of large breaches. Notice not required if the entity determines after a good faith investigation that misuse of the data has not or is not reasonably likely to occur. An entity that must notify more than 1,000 persons at one time of a security breach is required to also promptly notify all consumer reporting agencies of the breach. Entities subject to Title V of the GLBA are exempt. Exemption for good-faith acquisition by an employee or agent, so long as PI not used or subject to further willful unauthorized disclosure.	Statute not applicable if the personal data that was lost, stolen, or accessed by an unauthorized individual is encrypted, redacted or secured by any other method rendering it unreadable or unusable.	Entities regulated by state or federal law that maintain procedures for addressing security breaches pursuant to those laws are exempt. Third party notification: If covered entity maintains computerized data including PI that entity does not own or license, the entity shall give notice to and cooperate with the owner or licensee of the information of any breach immediately following discovery, if misuse or PI about a CO resident occurred or is likely to occur. Cooperation includes sharing with the owner or licensee information relevant to the breach, except that such cooperation shall not be deemed to require the disclosure of confidential business information or trade secrets.			No. Enforcement by Attorney General only.

MINTZ LEVIN

State and Bill Number	Data and consumers protected/Definition of Breach	Covered entities	Notice Procedures/ Timing/Exemptions	Encryption Safe Harbor	General & Preemption	Other provisions	Penalties	Private Cause of Action
Connecticut Conn. Gen Stat. 36a-701(b)	Personal information of Connecticut residents. Security Breach: Unauthorized access to or acquisition of electronic files, media, databases, or computerized data containing PI when access to the PI has not been secured by encryption or by any other method or technology that renders the PI unreadable or unusuable.	Any person who conducts business in Connecticut, and who, in the ordinary course of such person's business, owns licenses or maintains computerized data that includes personal information.	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 means prescribed in the statute allowed in the case of very large breaches. Notice not required if the entity responsible for the data determines in consultation with federal, state and local law enforcement agencies that there is no reasonable likelihood of harm to consumers.	Statute not applicable if the personal data that was lost, stolen, or accessed by an unauthorized individual is secured by encryption or by any other method or technology that renders it unreadable or unusable	Any person that maintains a security breach procedure pursuant to the rules, regulations, procedures or guidelines established by the primary or functional regulator is exempt.	Consumers have the right to place a "security freeze" on their credit reports. Third party notification: If a covered entity maintains computerized data that includes PI that the entity does not own, the entity must notify the owner or licensee of the information of any breach of security immediately following discovery if the PI was, or is reasonably believed to have been, accessed by an unauthorized person.	Failure to comply with statute constitutes an unfair trade practice.	No. Enforcement by Attorney General only.
Bulletin IC-25	Personal health and/or financial information of a Connecticut insured	All entities regulated by the Insurance Department of the State of Connecticut	Written notice to the Insurance Commissioner (email permissible) as soon as the incident is identified **but no later than five (5) calendar days after the incident is identified.**	NONE		An information security incident at a vendor or business associate of an entity regulated by the Insurance Department which has the potential of affecting a Connecticut insured should be reported by the licensee or registrant to the Commissioner.	Case-by-case basis that may result in administrative penalties	

MINTZ LEVIN

State and Bill Number	Data and consumers protected/Definition of Breach	Covered entities	Notice Procedures/ Timing/Exemptions	Encryption Safe Harbor	General & Preemption	Other provisions	Penalties	Private Cause of Action
Delaware H.B. 116 Del. C., Tit. 6, Chapter 12B, §§ 101-104	Personal information of Delaware residents. **Definition of "personal information" includes medical information.** Security Breach: An unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality or integrity of PI.	An individual or a commercial entity that conducts business in Delaware and owns or licenses computerized data that includes personal information.	Written or electronic 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 means prescribed in the statute allowed in the case of large breaches. Notice not required if the entity responsible for the data concludes that the breach will not likely result in harms to consumers. Prompt, written notification of the nature and circumstances of the breach must also be provided to the Consumer Protection Division of the Department of Justice.	Statute not applicable if the personal data that was lost, stolen, or accessed by an unauthorized individual is encrypted.	Entities regulated by any state or federal law that provides greater protection to personal information are exempt. Exemption for good-faith acquisition by an employee or agent, so long as PI not used or subject to further willful unauthorized disclosure.	Third party notification: If a covered entity maintains computerized data that includes PI that the entity does not own, the entity must notify the owner or licensee of the information of any breach of security immediately following discovery.	Appropriate penalties and damages may be assessed in an enforcement action brought by the Attorney General.	Yes. Plaintiff may recover treble damages and reasonable attorney fees.

MINTZ LEVIN

State and Bill Number	Data and consumers protected/Definition of Breach	Covered entities	Notice Procedures/ Timing/Exemptions	Encryption Safe Harbor	General & Preemption	Other provisions	Penalties	Private Cause of Action
Florida H.B. 481 Fl. Stat. Tit. XLVI, Ch. 817, §5681	Personal information of Florida residents. Security Breach: An unlawful and unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of PI.	Any person who conducts business in Florida and maintains computerized data in a system that includes personal information.	Written or electronic notice must be provided to victims of a material security breach **no later than 45 days following the determination of the breach.** The notification procedures must be consistent with the legitimate needs of law enforcement. If data was held by a person for another business entity, then notification to the business entity must be given within 10 days. Substitute notice by means prescribed in the statute allowed in the case of very large breaches. An entity that must notify more than 1,000 persons at one time of a security breach is required to also promptly notify all consumer reporting agencies of the breach. Notice not required if the entity responsible for the data concludes after a reasonable investigation or consultation with federal, state and local law enforcement agencies that the breach will not likely result in harm to consumers. Such a determination must be documented in writing and the documentation must be kept for five (5) years.	Statute not applicable if the personal data that was lost, stolen, or accessed by an unauthorized individual is encrypted.	Entities subject to federal data security regulations are exempt. Exemption for good-faith acquisition by an employee or agent, so long as PI not used for a purpose unrelated to the business or subject to further unauthorized use.	Third party notification: If a covered entity maintains computerized data that includes PI that the entity does not own, the entity must notify the owner or licensee of the information of any breach of security as soon as practicable following discovery, **but no later than 10 days following the determination** if the PI was, or reasonably believed to have been acquired by an unauthorized person.	For failure to provide notice of the security breach within 45 days: $1,000 per day per breach – not per individual affected by breach - , then up to $50,000 for each 30-day period up to 180 days, not to exceed $500,000. For failure to document and maintain written documentation of the investigation for five (5) years: an administrative fine in the amount of up to $50,000. Penalties do not apply to government agencies, unless the agencies entered into an agreement with contractors or third-party administrators to provide governmental services.	No. Allows the Department of Legal Affairs to assess and collect the fines.

MINTZ LEVIN

State and Bill Number	Data and consumers protected/Definition of Breach	Covered entities	Notice Procedures/ Timing/Exemptions	Encryption Safe Harbor	General & Preemption	Other provisions	Penalties	Private Cause of Action
Georgia S.B. 230 Ga. Code Ann., tit. 10, ch. 1, §910 thru 912	Personal information of Georgia residents. Definition of "personal information" includes (1) a social security number, (2) a driver's license number or state identification card number; (3) a financial account information number; or (4) a password, if any of these data elements alone would be sufficient to perform or attempt to perform identity theft against the person whose information was compromised. Security Breach; An unauthorized acquisition of an individual's electronic data that compromises the security, confidentiality, or integrity of PI.	Any information broker that maintains computerized data that includes personal information. "Information broker" defined as "any person or entity who, for monetary fees or dues, engages in whole or in part 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, but does not include any governmental agency whose records are maintained primarily for traffic safety, law enforcement, or licensing purposes."	Written or electronic notice must be provided to victims of a security breach within the most expedient time possible and without unreasonable delay, unless disclosure impedes a criminal investigation. If information is being held by another entity, notice by the holding entity to the owner entity must be given immediately after the breach. Substitute notice by means prescribed in the statute allowed in the case of very large breaches or if the information broker does not have sufficient contact information to notify affected individuals A data broker that must notify more than 10,000 individuals at one time of a security breach is required to also promptly notify all consumer reporting agencies of the breach. Exemption for good-faith acquisition by an employee or agent, so long as PI not used or subject to further willful unauthorized disclosure.	Statute not applicable if the personal data that was lost, stolen, or accessed by an unauthorized individual is encrypted.		Notice to other entities is required within 24 hours of discovery of the breach if the PI was, or is reasonably believed to have been acquired by an unauthorized person. Exemption for good-faith acquisition by an employee or agent, so long as PI not used or subject to further willful unauthorized disclosure.		No.

MINTZ LEVIN

State and Bill Number	Data and consumers protected/Definition of Breach	Covered entities	Notice Procedures/ Timing/Exemptions	Encryption Safe Harbor	General & Preemption	Other provisions	Penalties	Private Cause of Action
Hawaii SB 2290 Hawaii Rev. Stat. Tit. 26/Act 135	Personal information of Hawaii residents. Person's first name or initial and last name combined with: SSN; driver's license or state ID #; acct #, credit or debit card #, combined with any required info that allows access to account; or any other financial info. **Statute covers paper records also.** Security Breach: Any unauthorized access to and acquisition of unencrypted or unredacted records or data containing PI. Any incident of unauthorized access to and acquisition of encrypted records or data containing PI along with the confidential process or key constitutes a security breach.	Any agency, individual, or commercial entity that conducts business in Hawaii and owns or licenses computerized data that includes PI or maintains such data of PI of residents of Hawaii.	**Specific notice requirements.** Notice only required where illegal use of the PI has occurred or is reasonably likely to occur or that creates a material risk of harm to the person. Notices must include descriptions of the security breach. Allows substitute notice if more than 200,000 people affected, or would cost more than $100,000. Must notify credit reporting agencies if more than 1,000 people are affected. **If more than 1,000 persons are notified at one time under this section, notification to Hawaii's Office of Consumer Protection is required.** Exemption for good-faith acquisition by an employee or agent, so long as PI not used for a purpose other than a lawful purpose of the business and is not subject to further unauthorized disclosure.	Statute not applicable if the personal data that was lost, stolen, or accessed by an unauthorized individual is encrypted.	Entities regulated by state or federal law that maintain procedures for addressing security breaches pursuant to those laws are exempt. Waiver not permitted.	Notice to other entities is required immediately following the breach.	At most $2,500 per violation and for any actual damages faced by an individual.	No.

MINTZ LEVIN

State and Bill Number	Data and consumers protected/Definition of Breach	Covered entities	Notice Procedures/ Timing/Exemptions	Encryption Safe Harbor	General & Preemption	Other provisions	Penalties	Private Cause of Action
Idaho Idaho Code §§ 28-51-104 to 28-51-107 **Amended by H.B. 566**	Personal information of Idaho residents. Security Breach: An illegal acquisition of unencrypted computerized data that materially compromises the security, confidentiality, or integrity of PI for one or more persons.	An agency, individual or a commercial entity that conducts business in Idaho and owns or licenses computerized data that includes personal information about a resident of Idaho.	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 means prescribed in the statute allowed in the case of larger breaches. Notification required solely in the case of breaches that "materially compromise the security, the security, confidentiality, or integrity of personal information for one (1) or more persons maintained by an agency, individual or a commercial entity." Must notify the AG within 24 hours for certain security breaches as required by statute. H.B. 566 Exemption for good-faith acquisition by an employee or agent, so long as PI not used or subject to further unauthorized disclosure.	Statute not applicable if the personal data that was lost, stolen, or accessed by an unauthorized individual is encrypted.	Entities regulated by state or federal law that maintain procedures for addressing security breaches pursuant to those laws are exempt.	Notice to third party entities required if misuse of PI about an ID resident occurred or is likely to occur. Cooperation includes sharing with the owner or licensee information relevant to the breach.	Fine of not more than twenty-five thousand dollars ($25,000) per breach of the security of the system for any covered entity that intentionally fails to give notice. Any governmental employee that intentionally discloses personal information not subject to disclosure otherwise allowed by law, is guilty of a misdemeanor and, upon conviction thereof, shall be punished by a fine of not more than two thousand dollars ($2,000), or by imprisonment in the county jail for a period of not more than one (1) year, or both. H.B. 566	No. Enforcement action brought by an agency's, commercial entity's or individual's primary regulator. " 'Primary regulator' of a commercial entity or individual licensed or chartered by the United States is that commercial entity's or individual's primary federal regulator, the primary regulator of a commercial entity or individual licensed by the department of finance is the department of finance, the primary regulator of a commercial entity or individual licensed by the department of insurance is the department of insurance and, for all agencies and all other commercial entities or individuals, the primary regulator is the attorney general."

State and Bill Number	Data and consumers protected/Definition of Breach	Covered entities	Notice Procedures/ Timing/Exemptions	Encryption Safe Harbor	General & Preemption	Other provisions	Penalties	Private Cause of Action
Illinois H.B. 1633 Ill. Comp. Stat., 815 ILCS 530/1 et seq. Amended by House Bill 3025, effective January 1, 2012	Personal information of Illinois residents. Security Breach: An unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of PI. NOTE: Illinois may take the position that any unauthorized acquisition or use by a third party triggers the notification obligation, regardless of materiality or ownership of the data.	Any data collector that owns or licenses personal information concerning a resident of Illinois. "Data collector" definition includes, but is not limited to "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." Effective 1/1/2012 – expands reach to include service providers who maintain or store but do not own or license PI. Service provider must cooperate with the data owner or licensor with respect to breaches of PI in the service provider's care	Written or electronic notice must be provided to victims of a security breach within the most expedient time possible and without unreasonable delay. Substitute notice by means prescribed in the statute allowed in the case of very large breaches. **Any data collector that owns or licenses personal information shall notify the Attorney General of a breach. H.B. 5708** Exemption for good-faith acquisition by an employee or agent, so long as PI not used or subject to further unauthorized disclosure. **Effective 1/1/2012 – Specific Notice Content required – notices must include contact information for credit reporting agencies and the Federal Trade Commission, along with a "statement that the individual can obtain information from these sources about fraud alerts and security freezes."**	Statute not applicable if the personal data that was lost, stolen, or accessed by an unauthorized individual is encrypted or redacted.	Waiver not permitted	Effective 1/1/2012: standards for disposing of material containing PI in a manner that renders the PI unreadable, unusable and undecipherable.	A violation of the statute constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act.	No.

MINTZ LEVIN

State and Bill Number	Data and consumers protected/Definition of Breach	Covered entities	Notice Procedures/ Timing/Exemptions	Encryption Safe Harbor	General & Preemption	Other provisions	Penalties	Private Cause of Action
Indiana S.B. 503 (government agencies only) Ind. Code, tit. 24, art. 4.9	Personal information of Indiana residents.	Any state agency that owns or licenses computerized data that includes personal information.	Written or electronic 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 means prescribed in the statute allowed in the case of very large breaches. If an agency is required to provide notice under this section to more than 1,000 persons, the state agency must also promptly notify all consumer reporting agencies	Statute not applicable if the personal data that was lost, stolen, or accessed by an unauthorized individual is encrypted.				No.

MINTZ LEVIN

State and Bill Number	Data and consumers protected/Definition of Breach	Covered entities	Notice Procedures/ Timing/Exemptions	Encryption Safe Harbor	General & Preemption	Other provisions	Penalties	Private Cause of Action
Indiana H.B. 1101 Ind. Code §§ 24-4.9 et seq., 4-1-11 et seq., 2009 H.B. 1121	Personal information of Indiana residents. **Covers non-electronic information if it was originally computerized data.** **NOTE: Definition includes a SSN, standing alone without a name that is not redacted or encrypted.** **Security Breach: An unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of PI. Term includes the unauthorized acquisition of computerized data that has been transferred to another medium, including paper, microfilm or a similar media, even if the transferred data are no longer in a computerized format.**	Any company owning or using computerized "personal information of an Indiana resident for commercial purposes."	Written, electronic, telephonic or facsimile 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 or jeopardizes national security. Substitute notice by means prescribed in the statute allowed in the case of very large breaches. Exemption for good-faith acquisition by an employee or agent, so long as PI not used or subject to further unauthorized disclosure. Definition of "breach of the security system" does not include the "unauthorized acquisition of a portable electronic device on which personal information is stored if access to the device is protected by a password that has not been disclosed"	Statute applies to both unencrypted and encrypted personal information acquired by an unauthorized person. "Encrypted" is defined as (1) the transformation of data through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key; or (2) securing data through another method that renders the personal information unreadable or unusable. "Redacted" is defined as altering or truncating personal information so that not more than the last four digits of: (1) a social security number; (2) a driver's license number; (3) a state identification number; or (4) an account number; is accessible as part of personal information.	Entities subject to and in compliance with certain federal data security laws and regulations specified in the present statute are exempt.	Entities responsible for personal data are required to also notify each consumer reporting agency of the security breach.	The attorney general may bring an action o obtain any or all of the following: (1) an injunction to enjoin future violations of the statute (2) a civil penalty of not more than one hundred fifty thousand dollars ($150,000) per deceptive act; (3) the attorney general's reasonable costs in: (a) the investigation of the deceptive act; and (b) maintaining the action; (4) reasonable attorney's fees, and (5) costs of the action.	No.

State and Bill Number	Data and consumers protected/Definition of Breach	Covered entities	Notice Procedures/ Timing/Exemptions	Encryption Safe Harbor	General & Preemption	Other provisions	Penalties	Private Cause of Action
Iowa S.F. 2308 Iowa Code § § 715C.1 (2008 S.F. 2308)	Personal information of Iowa residents. **PI definition includes biometric data or unique electronic identifier.**	Any person who owns or licenses computerized data that includes a consumer's personal information that is used in the course of the person's business, vocation, occupation, or volunteer activities. Any person who maintains or otherwise possesses personal information on behalf of another person. The definition of "person" includes governmental subdivisions, agencies, or instrumentalities.	**Specific notice content requirements.** Written or electronic notice must be given to any consumer whose personal information was included in the information that was breached in the most expeditious manner possible and without unreasonable delay, unless a law enforcement agency determines that notification will impede a criminal investigation and the agency has made a written request that the notification be delayed. Notice must include (1) a description of the breach of security; (2) approximate date of the breach; (3) type of personal information obtained as a result of the breach; (4) contact information for consumer reporting agencies; (5) advice to the consumer to report suspected identity theft to local law enforcement or the AG. Substitute notice by means prescribed in the statute allowed in the case of very large breaches. Notice not required if the breached entity determines after appropriate investigation or after consultation with relevant federal, state, or local agencies responsible for law enforcement, that no reasonable likelihood of financial harm to the consumers whose personal information has been acquired has resulted or will result from the breach. Such a determination must be documented in writing and the documentation must be maintained for five years.	Statute not applicable if the personal data that was breached was encrypted, redacted, or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable. "Encryption" is defined as "the use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without the use of a confidential process or key." "Redacted" is defined as "altered or truncated so that no more than five digits of a social security number or the last four digits of other numbers designated in section 715A.8,subsection 1, paragraph "a", is accessible as part of the data."	Statute does not apply to a person that : (1) complies with notification requirements or breach of security procedures established by a person's primary or functional federal regulator or by a state or federal law that provides greater protection to personal information and at least as thorough disclosure requirements for breach of security or personal information than that provided by this statute, and (2) is subject to and in compliance with Title V of the GLBA.		Attorney general may seek and obtain an order that a party held to violate this section pay damages to the Attorney General on behalf of a person injured by the violation.	No.

MINTZ LEVIN

State and Bill Number	Data and consumers protected/Definition of Breach	Covered entities	Notice Procedures/ Timing/Exemptions	Encryption Safe Harbor	General & Preemption	Other provisions	Penalties	Private Cause of Action
Kansas S.B. 196 K.S.A. 50-7a01 et seq.	Personal information of Kansas residents, including account number or credit card/debit card number, **alone or in combination with** any required security code, access code or password that would permit access to a consumer's financial account. **Security Breach**: Any unauthorized access to and acquisition of unencrypted or redacted computerized data that compromises the security, confidentiality, or integrity of PI and that causes, or entity reasonably believes has caused or will cause, identity theft to any consumer.	A person that conducts business in Kansas, or a government, governmental subdivision or agency that owns or licenses computerized data that includes personal information.	Written or electronic notice must be provided to victims of a security breach within the most expedient time possible and without unreasonable delay, unless disclosure impedes a criminal investigation. Substitute notice by means prescribed in the statute allowed in the case of large breaches. An entity that must notify more than 1,000 consumers at one time of a security breach is required to also promptly notify all consumer reporting agencies of the breach. Notification not required if after a good-faith, reasonable and prompt investigation the entity determines that the PI has not been and will not be misused.	Statute not applicable if the personal data that was lost, stolen, or accessed by an unauthorized individual is encrypted or redacted. "Encrypted" defined as the "transformation of data through the use of algorithmic process into a form in which there is a low probability of assigning meaning without the use of a confidential process or key, or securing the information by another method that renders the data elements unreadable or unusable." "Redacted" is defined as the "alteration or truncation of data" so that no more than the (a) five digits of a social security number, or (b)the last four digits of a driver's license number, state identification number or account number are accessible as part of the personal information.	Entities regulated by state or federal law that maintain procedures for addressing security breaches pursuant to those laws are exempt.	Enforcement actions against insurance companies licensed to do business in Kansas may only be brought by the insurance commissioner. Notice to other entities required.	Appropriate penalties and damages may be assessed in an enforcement action brought by the Attorney General.	No.

MINTZ LEVIN

State and Bill Number	Data and consumers protected/Definition of Breach	Covered entities	Notice Procedures/ Timing/Exemptions	Encryption Safe Harbor	General & Preemption	Other provisions	Penalties	Private Cause of Action
Louisiana S.B. 205 La. Rev. Stat., ch. § 51:3071 et seq	Personal information of Louisiana residents.	Any person or agency that conducts business in Louisiana or that owns or licenses computerized data that includes personal information.	Written or electronic 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 means prescribed in the statute allowed in the case of very large breaches. Notice not required if the entity responsible for the data concludes after a reasonable investigation that there is no reasonable likelihood of harm to consumers. Notice to AG Required: Covered entity must provide written notice to the Consumer Protection Section, including details of breach, names of all LA citizens affected by the breach. Shall be timely received if within 10 days of distribution of notice to LA citizens.	Statute not applicable if the personal data that was lost, stolen, or accessed by an unauthorized individual is encrypted or redacted.	Financial institutions subject to and in compliance with the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice are exempt.	Notice to other entities required.	Failure to provide timely notice punishable by a fine not to exceed $5,000 per violation. Notice to state AG shall be "timely" if received within 10 days of distribution of notice to LA citizens. Each day notice is not received by AG is deemed a separate violation.	Yes. Civil action to recover actual damages.

State and Bill Number	Data and consumers protected/Definition of Breach	Covered entities	Notice Procedures/ Timing/Exemptions	Encryption Safe Harbor	General & Preemption	Other provisions	Penalties	Private Cause of Action
Maine L.D. 1671 Me. Rev. Stat. Tit. 10, ch. 210-B, §§1346-1349 Amended by L.D. 70, eff. Sept 13, 2009	Personal information of Maine residents. Definition of "personal information" includes (1) a social security number, (2) a driver's license number or state identification card number; (3) a financial account information number; or (4) a password, if any of these data elements alone would be sufficient to permit a person to fraudulently assume or attempt to assume the identity of the person whose information was compromised. Includes unauthorized acquisition, release or use of PI. Security Breach: An unauthorized acquisition, release or use of an individual's computerized data that contains PI that compromises the security, confidentiality or integrity of the PI.	All private sector businesses (added to regs Jan. 1, 2007). Information brokers that maintain computerized data containing personal information. "Information broker" defined as "a person who, for monetary fees or dues, engages in whole or in part 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 3rd parties." The definition does not include "a governmental agency whose records are maintained primarily for traffic safety, law enforcement or licensing purposes."	Written or electronic notice must be provided to victims of a security breach. Entities may not delay notification to Maine residents any longer than **seven business days** after a law enforcement agency determines that notification will not compromise a criminal investigation. Substitute notice by means prescribed in the statute allowed if the cost of providing notice exceeds $5,000, the affected class exceeds 1,000 or the data broker does not have sufficient contact information. A data broker that must notify more than 1,000 persons at one time of a security breach is required to also promptly notify all consumer reporting agencies of the breach, as prescribed in the statute. The data broker must also notify the appropriate state regulators within the Department of Professional and Financial Regulation (data brokers) or alternatively, the Attorney General. Notice not required if security software to block unauthorized transactions does not show improper activity after the security breach.	Statute not applicable if the personal data that was lost, stolen, or accessed by an unauthorized individual is encrypted or redacted. "Encryption" defined as "the disguising of data using generally accepted practices.	Entities covered by Title V of the GLBA that maintain procedures to block unauthorized transactions are exempt. Good-faith acquisition, release or use by employee acting on behalf of entity is not breach if PI is not used or subject to further unauthorized disclosure to another person	The statute is enforced by the Department of Professional and Financial Regulation as to licensed data brokers and by the Attorney General as to all other brokers. Notice to other entities required.	Fines of not more than $500 per violation, up to a maximum of $2500 per each day; equitable relief; enjoinment from future violations.	No.

MINTZ LEVIN

State and Bill Number	Data and consumers protected/Definition of Breach	Covered entities	Notice Procedures/ Timing/Exemptions	Encryption Safe Harbor	General & Preemption	Other provisions	Penalties	Private Cause of Action
Maryland S.B. 486 Md. Code, Com. Law § 14-3501 et seq.	Personal information of Maryland residents, including an individual Taxpayer Identification Number. Security Breach: The unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of the PI. Good-faith acquisition, release or use by employee acting on behalf of entity is not breach if PI is not used or subject to further unauthorized disclosure to another person	Any business that owns or licenses personal information of an individual residing in Maryland, and any business that uses a nonaffiliated third party as a service provider to perform services for the business and discloses personal information about an individual residing in Maryland under a written contract with the third party must require by contract that the third party implement and maintain reasonable security procedures and practices.	Notice shall be given as soon as reasonably practicable after the business discovers or is notified of the breach of the security of a system, unless a law enforcement agency determines that the notification will impede a criminal investigation or jeopardize homeland or national security, or to determine the scope of the breach of the security of a system, identify the individuals affected, or restore the integrity of the system. Notice may be given by written notice, by electronic mail if the individual has expressly consented to receive electronic notice; or the business conducts its business primarily through the Internet, by telephonic notice, or by substitute notice by means prescribed in the statute allowed in the case of very large breaches. **Specific notice content requirement:** Notice must include a description of the categories of information breached, contact information for the Attorney General, Federal Trade Commission, and Credit Reporting Agencies. **Prior to giving the notification required this section a business shall provide notice of a breach of the security of a system to the Office of the Attorney General.**	Statute applies only to unencrypted personal information acquired by an unauthorized person. "Encrypted" means the transformation of data through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key.	A business that is subject to and in compliance with § 501(b) of the GLBA, § 216 of the federal Fair and Accurate Transactions Act, 15 U.S.C. § 1681w, shall be deemed to be in compliance with the statute. PI does not include information disseminated or listed in accordance with HIPAA.	Statute requires reasonable security procedures and practices that are appropriate to the nature of the personal information owned or licensed and the nature and size of the business and its operations. Compliance cannot be waived.	A violation of the statute implicates Title 13 of the Maryland Code, the Unfair and Deceptive Trade Practices Act. Appropriate penalties and damages may be assessed in an enforcement action brought by the Attorney General.	Yes, consumers may bring actions under Title 13 of the Maryland Code, the Unfair and Deceptive Trade Practices Act.

MINTZ LEVIN

State and Bill Number	Data and consumers protected/Definition of Breach	Covered entities	Notice Procedures/ Timing/Exemptions	Encryption Safe Harbor	General & Preemption	Other provisions	Penalties	Private Cause of Action
Massachusetts Mass. Gen. Laws § 93H-1 et seq. **Proposed amendements set aside for study. H.B. 326 (relates to identity theft) H.B. 3427 (relates to identity theft protection)**	Personal information of Massachusetts residents. Personal information is defined as first name or initial and last name combined with one of the following: SSN, driver's license, state i.d. card number, passport, and financial account information with or without password or security code information. **Includes non-electronic personal information.** Security Breach: An unauthorized acquisition or unauthorized use of unencrypted data or encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality or integrity of PI.	State agencies, commissions, bureaus etc. and persons, corporations associations, partnerships or other legal entity that maintains, stores, owns or licenses data that includes personal information about a resident of Massachusetts.	**Specific notice requirements.** Entities that maintain or store but do not own personal information must provide notice to, and cooperate with, the entity that owns or leases the data. The entity that owns or leases the data must provide notice as soon as possible and without unreasonable delay to the attorney general , the director of consumer affairs and business regulation and to affected residents. Notification to affected residents cannot include the nature of the breach or unauthorized acquisition or the number of residents of Massachusetts affected by the breach. Notice to affected residents must include (1) consumer's right to obtain a police report; (2) how a consumer requests a security freeze; and (3) fees required to be paid to any of the consumer reporting agencies. Notice may be delayed if provision of such notice will impede a criminal investigation. Notice may be written or electronic. Substitute notice permitted if cost of notice will exceed $250,000 or the affected class of residents is greater than 500,000.	Covers unencrypted data or the acquisition of the confidential process or key that is capable of compromising the security and confidentiality of encrypted data. NOTE: Massachusetts may require notice to the AG even in cases where security breach involves encrypted data. Entity must be able to determine that key or confidential process has not been compromised as part of the incident.	An entity is considered in compliance with the **statute** if the entity follows a federal law regarding protection or privacy of information and the entity notifies MA residents pursuant to the federal law. M.G.L. c. 93H, §5. **Please note that this does not apply to 201 C.M.R. 17.00.**	Disposal Law – 93- I When disposing of records: paper records containing personal information must be redacted, burned, pulverized or shredded. Electronic data containing personal information shall be destroyed or erased. Notice to other entities required. Cooperation includes, but is not limited to: (i) informing the licensor or owner of the breach; (ii) the data or approximate date of such incident and the nature of the incident; (iii) any steps that entity has taken or plans to take relating to the incident, except that such cooperation shall not require the disclosure of confidential information or trade secrets.	The Massachusetts Attorney General may bring an action under Chapter 93A, the Commonwealth's consumer protection statute, which permits the imposition of significant fines, injunctive relief, and attorneys' fees. (93H § 6) A civil penalty of $5,000 may be awarded for each violation. (93A § 4) Businesses can be subject to a fine of up to $50,000 for each instance of improper disposal of data. (93I § 3)	Yes. Massachusetts consumers may seek damages under Chapter 93A, which in some cases, may be trebled.

State and Bill Number	Data and consumers protected/Definition of Breach	Covered entities	Notice Procedures/ Timing/Exemptions	Encryption Safe Harbor	General & Preemption	Other provisions	Penalties	Private Cause of Action
Regulation: 201 CMR 17.00 General compliance deadline: March 1, 2010 Revised Regulations	"Personal information" means a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that "Personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.	Every person that owns, licenses, stores or maintains personal information about a resident of Massachusetts. "Person" means a natural person, corporation, association, partnership or other legal entity, other than an agency, executive office, department, board, commission, bureau, division or authority of the Commonwealth, or any of its branches, or any political subdivision thereof. Covers third-party service providers with access to personal information. Requires entities to collect and store the minimum amount of personal information necessary to accomplish the legitimate purpose for which it was collected, and requires entities to restrict access to the personal information to the smallest possible number of users.		The regulations require the encryption of all transmitted records and files containing personal information, including those in wireless environments, which will travel across public networks. For files containing personal information on a system that is connected to the Internet, there must be firewall protection with up-to-date patches, including operating system security patches.	None.	The regulations require the development, implementation, maintenance and monitoring of a comprehensive information security program consistent with industry standards that is applicable to any records containing such personal information. Whether the comprehensive information security program (called for by the statute) is in compliance with these regulations for the protection of personal information, whether pursuant to section 17.03 or 17.04 hereof, shall be evaluated taking into account (i) the size, scope and type of business of the person obligated to safeguard the personal information under such comprehensive information security program, (ii) the amount of resources available to such person, (iii) the amount of stored data, and (iv) the need for security and confidentiality of both consumer and employee information.	Please see above for a summary of applicable penalty provisions of Mass. Gen. Laws. c. 93A, c. 93H and c. 93I.	Please see above. Consumers may seek damages under Mass. Gen. Laws. c. 93A.

MINTZ LEVIN

State and Bill Number	Data and consumers protected/Definition of Breach	Covered entities	Notice Procedures/ Timing/Exemptions	Encryption Safe Harbor	General & Preemption	Other provisions	Penalties	Private Cause of Action
Michigan S.B. 309 Mich. Comp.. Law § 445.72	Personal information of Michigan residents. Person's first name or initial and last name combined with: SSN; driver's license or state ID #; acct #, credit or debit card #, combined with any required info that allows access to account; or any other financial info. Security Breach: The unauthorized access and acquisition of data that compromises the security or confidentiality of PI maintained by a covered entity as part of a database of PI regarding multiple individuals A good-faith but unauthorized acquisition of PI by an employee or other individual, where the access was related to the activities of the covered entity, is not a breach of security unless the PI is misused or disclosed to an unauthorized person. In making this determination, a covered entity shall act with the care an ordinarily prudent entity in a like position would exercise under the circumstances.	State agencies including institutions of higher education; individual, partnership, corporation, limited liability company, association or other legal entity that owns or licenses personal information.	**Specific notice content required.** Notice required without unreasonable delay unless determination that breach has not or is not likely to cause substantial loss or injury to, or result in, identity theft with respect to one or more residents of the state. Notice may be by mail, email or telephone depending on existing business relationship with recipient. Substitute notice permitted if the cost of providing notice will exceed $250,000 or notice must be provided to more than 500,000 residents. Notice must be written in a clear and conspicuous manner and (1) describe the security breach in general terms; (2) describe the type of Personal Information that is the subject of the unauthorized access or use; (3) generally describe what the agency or person providing the notice has done to protect the information from future breaches; (4) include a telephone number where a recipient of the notice may obtain assistance or additional information; and (5) remind recipients of the need to remain vigilant for incidents of fraud and identity theft. Must be communicated if notice is provided via telephone.	Statute not applicable if the personal data that was lost, stolen, or accessed by an unauthorized individual is encrypted.	Financial institutions and entities covered by HIPAA are exempt.	Notice to other entities is required. Covered entities may deliver notice pursuant to an agreement with another covered entity, if the agreement does not conflict with MI law. Proposed Legislation : S.B. 149 – Prohibits obtaining information over the internet by false pretenses S.B. 717 – provides the standards for safeguarding PI ; provides for civil immunity.	Civil penalty for failure to provide notice of not more than $250 for each failure to provide notice, capped at $750,000 per security breach. Penalties do not affect availability of civil remedies under state or federal law. Criminal penalties for notice of a security breach that has not occurred, where such notice is given with the intent to defraud. Misdemeanor – 30 days imprisonment or fine of $250 (or both) for each violation	No.

State and Bill Number	Data and consumers protected/Definition of Breach	Covered entities	Notice Procedures/ Timing/Exemptions	Encryption Safe Harbor	General & Preemption	Other provisions	Penalties	Private Cause of Action
Minnesota H.F. 225 H. F. 2121 Minn. Stat. §§ 325E.61, 325E.64	Personal information of Minnesota residents. Security Breach: An unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of PI. Good-faith acquisition, release or use by employee or agent for purposes of entity is not breach if PI is not used or subject to further unauthorized disclosure	State agencies (HF 225). Any person or business doing business in Minnesota that owns or licenses computerized data containing personal information (H.F. 2121).	Entities doing business in Minnesota must provide written or electronic notice 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 means prescribed in the statute allowed in the case of very large breaches.	Statute not applicable if the personal data that was lost, stolen, or accessed by an unauthorized individual is encrypted.	Financial institutions and entities covered by HIPAA are exempt.	Definition of "breach" does not include loss of a portable electronic device containing password protected personal information. Notice to other entities required. Waiver not permitted.		Yes.
Mississippi H.B. 583 Reg. Sess. (MI 2010)	Personal Information of a Mississippi resident. Does not include publicly available information that is lawfully made available to the general public from federal, state or local government or widely distributed media. Security Breach: An unauthorized acquisition of electronic file, media, databases of computerized data containing PI when access to the PI has not been secured by encryption or by any other method of technology that renders the PI unreadable or unusable.	Any person who conducts business in Mississippi and who, in the ordinary course of the person's business functions, owns, licenses or maintains computerized personal information of any state resident and discovers a security breach in a database it owns or licenses, or that receives notice of a security breach	Without unreasonable delay, subject to completion of an investigation to determine nature and scope of breach, identify affected individuals and restore reasonable integrity of systems. May be delayed on law enforcement request. Substitute notice by means prescribed in the statute allowed in cases of large breaches.	Statute not applicable if the database was encrypted unless acquired in an encrypted form by a person with unauthorized access to the encryption key.		**Exception for "no harm" determination.** Notification is not required if, after the investigation, the person reasonably determines that the breach will not likely result in harm to the affected individual. Persons that maintain computerized data owned by others that includes Personal Information must give notice to the owner or licensee of the information of any breach following discovery of the breach if the Personal Information may have been acquired by an unauthorized person.	Failure to comply is a violation of state's unfair trade practice law and AG has exclusive enforcement authority.	No.

State and Bill Number	Data and consumers protected/Definition of Breach	Covered entities	Notice Procedures/ Timing/Exemptions	Encryption Safe Harbor	General & Preemption	Other provisions	Penalties	Private Cause of Action
Missouri Mo. Rev. Stat. § 407.1500 (2009 H.B. 62)	Personal information of Missouri residents, including unique electronic identifier or routing code in combination with required security code or access code. Also includes medical and health insurance information, including an individual's medical history, mental or physical condition, treatment or diagnosis, health insurance policy number and any other unique identifier used by a health insurer. Security Breach: Unauthorized access to and unauthorized acquisition of PI maintained in computerized form that compromises the security, confidentiality or integrity of the PI. Good-faith acquisition, release or use by employee or agent for purposes of entity is not breach if PI is not used or subject to further unauthorized disclosure	State agencies. Any person or business that conducts business in Missouri that owns or licenses computerized data containing personal information.	Entities conducting business in Missouri must provide written or electronic notice to residents of Missouri when the security of their personal information has been compromised. Notice to the Missouri AG and national consumer credit reporting agencies if more than 1,000 Missouri residents are affected.	Notice not required if the personal information compromised was encrypted.	Entities regulated by state or federal law that maintain procedures for addressing security breaches pursuant to those laws are deemed to be in compliance. Entities that maintain its own notice procedures as part of an information security plan and whose notice procedures are consistent with the timing of the Missouri statute will be deemed in compliance if notice is provided in accordance with the information security plan.	"Material risk of harm" trigger - notice not required if, after an appropriate investigation or consultation with law enforcement authorities, the business determines that identity theft is not likely to result from the breach. Notice to other entities required.	Attorney General may seek actual damages and/or civil penalties (not to exceed $150,000 for each security breach) for failures to comply	No.

State and Bill Number	Data and consumers protected/Definition of Breach	Covered entities	Notice Procedures/ Timing/Exemptions	Encryption Safe Harbor	General & Preemption	Other provisions	Penalties	Private Cause of Action
Montana H.B. 732 Mont. Code § 30-14-1701 et seq., 2009 H.B. 155, Chapter 163	Personal information of Montana residents. Definition of "personal information" includes insurance policy number as well as a social security number alone. Security Breach: Any unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of PI and causes or is reasonably believed to cause loss or injury to a MT resident.	Any person or business that conducts business in Montana, and owns or licenses computerized data that includes personal information.	**Specific notice requirements.** Written, electronic or telephonic notice must be provided to victims of a security breach without unreasonable delay, unless disclosure impedes law enforcement investigation. Substitute notice by means specified in the statute allowed in the case of very large breaches. Notification required solely in the case of breaches that materially compromise the security, confidentiality, or integrity of personal information maintained by the person or business responsible for the data and causes or is reasonably believed to cause loss or injury to a Montana resident. If the notice provided suggests or implies that a consumer can obtain a copy of their file from a credit reporting agency, the business must coordinate with the credit reporting agency regarding the timing, content, and distribution of notice to the Montana consumer as long as the cooperation cannot unreasonably delay the notice.	Statute not applicable if the personal data that was lost, stolen, or accessed by an unauthorized individual is encrypted.		Entities responsible for personal data must destroy the data that is no longer necessary by shredding, erasing or modifying the data so that it becomes unreadable. Notice to other entities required.	Temporary and permanent injunction. Penalties for a violation of the statute are provided in 30-14-142.	No.

State and Bill Number	Data and consumers protected/Definition of Breach	Covered entities	Notice Procedures/ Timing/Exemptions	Encryption Safe Harbor	General & Preemption	Other provisions	Penalties	Private Cause of Action
Nebraska Neb. Rev. Stat. §§ 87-801, -802, -803, -804, -805, -806, -807	Personal information of Nebraska residents. Definition of "personal information" includes **biometric data: fingerprints, voiceprints, retina or iris images, DNA profiles and any other "unique physical representations."** **NOTE: Statute further limits PI definition to if either the name OR the data elements are not encrypted or redacted** Security Breach: An unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality or integrity of PI. Good-faith acquisition, release or use by employee or agent for purposes of entity is not breach if PI is not used or subject to further unauthorized disclosure Acquisition of PI pursuant to a search warrant, subpoena or court order or pursuant to a subpoena or order of a state agency not a breach.	Individual or commercial entity that conducts business in Nebraska and that owns or licenses computerized data which includes personal information.	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 means specified in the statute allowed in the case of very large breaches. Notification required solely in the case of breaches that "materially compromise the security, confidentiality or integrity of the personal information."	Statute not applicable if the personal data that was lost, stolen, or accessed by an unauthorized individual is encrypted or redacted. "Encrypted" is defined as "converted by use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without use of a confidential process or key." "Redact" is defined as altering or truncating data in a way that only the last fours digits of a social security number, driver's license number, state identification card or account number are accessible.	Entities regulated by state or federal law that maintain procedures for addressing security breaches pursuant to those laws are exempt.	Notice to other entities required. Waiver not permitted.		No.

State and Bill Number	Data and consumers protected/Definition of Breach	Covered entities	Notice Procedures/ Timing/Exemptions	Encryption Safe Harbor	General & Preemption	Other provisions	Penalties	Private Cause of Action
Nevada A.B. 334 S.B. 347 Nev. Rev. Stat. 603A.010 et seq.	Personal information of Nevada residents when the name and the data elements are not encrypted. Definition of "personal information" includes "unique biometric data," electronic signature, alien registration number, government passport number, employer id number, tax payer id number, Medicaid account number, food stamp account number, health insurance number, professional license numbers, and utility account number. Security Breach: An unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of PI. Good-faith acquisition, release or use by employee or agent for purposes of entity is not breach if PI is not used or subject to further unauthorized disclosure	Governmental agencies (A.B. 334) Data collectors (S.B. 347). "Data collectors" definition includes "government, businesses and associations who handle, collect, disseminate or otherwise deal with non public personal information."	Written or electronic 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 means specified in the statute allowed in the case of very large breaches. Notification required solely in the case of breaches that materially compromise the security, confidentiality or integrity of the personal information.	Statute not applicable if the personal data that was lost, stolen, or accessed by an unauthorized individual is encrypted.	Entities subject to and in compliance with the privacy and security provisions of Title V of the GLBA are exempt.	Entities responsible for personal data must take reasonable measures to destroy the data that is no longer necessary. **Entities responsible for personal data are also required to encrypt data that is being transmitted using encryption consistent with PCI DSS standards.** Notice to other entities required. Entities must maintain reasonable protections for PI Special rules applicable to electronic health records – see Nev. Rev. Stat. §439 Waiver not permitted		No.

MINTZ LEVIN

State and Bill Number	Data and consumers protected/Definition of Breach	Covered entities	Notice Procedures/ Timing/Exemptions	Encryption Safe Harbor	General & Preemption	Other provisions	Penalties	Private Cause of Action
Nev. Rev. Stat. Chapter 603A	Prohibits the transfer of "any personal information of a customer through an electronic transmission other than a facsimile to a person outside of the secure system of the business unless the business uses encryption to ensure the security of electronic transmission." Personal information includes a natural person's first name or first initial and last name in combination with any one or more of the following data elements, when the name and data elements are not encrypted: 1) Social Security number; 2) Driver's license number or identification card number; or 3) Account number, credit card number or debit card number, in combination with any required security code, access code or password that would permit access to the person's financial account.	Any business that owns or licenses computerized data that includes Personal Information of Nevada residents.	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 integrity and security of the system. For entities that maintain data owned by others, notice must be given to the owner of the data.	Statute not applicable if personal information transferred to a person outside of the secure system of the business is encrypted.	Personal information does not include the last four digits of a social security number or publicly available information that is lawfully made available to the general public.	**Requires compliance with PCI DSS under certain circumstances.** If a data collector doing business in this State accepts a payment card in connection with a sale of goods or services, the data collector shall comply with the current version of the Payment Card Industry (PCI) Data Security Standard, as adopted by the PCI Security Standards Council or its successor organization, with respect to those transactions, not later than the date for compliance set forth in the Payment Card Industry (PCI) Data Security Standard or by the PCI Security Standards Council or its successor organization.		No, but see exception. Data collectors who provide timely notice may bring actions for damages against a person that unlawfully obtained or benefited from Personal Information maintained by the data collector. Damages, costs of the action, attorneys' fees, costs of notification as well as punitive damages are recoverable.

MINTZ LEVIN

State and Bill Number	Data and consumers protected/Definition of Breach	Covered entities	Notice Procedures/ Timing/Exemptions	Encryption Safe Harbor	General & Preemption	Other provisions	Penalties	Private Cause of Action
New Hampshire HB 1660 N.H. Rev. Stat. §§ 359-C:19, -C:20, -C:21	Personal information of New Hampshire residents when either the name or the data elements are not encrypted. Person's first name or initial and last name combined with: SSN; driver's license or state ID #; acct #, credit or debit card #, combined with any required info that allows access to account; or any other financial info. Security Breach: An unauthorized acquisition of computerized data that compromises the security or confidentiality of PI Good-faith acquisition, release or use by employee or agent for purposes of entity is not breach if PI is not used or subject to further unauthorized disclosure	Any person that conducts business in NH and owns or licenses computerized data that includes PI or maintains such computerized data.	**Specific notice content required.** Notification as soon as possible is required if PI has been misused or is reasonably likely to be misused. Notice must be in writing, by telephone or in electronic form such as email. Substitute notice allowed when cost of providing notice would exceed $5,000 or affected class of individuals to be notified exceeds 1,000. Requires notification of CRA if notice provided to more than 1,000 people. Notice must include at a minimum (1) a description of the incident in general terms; (2) the approximate date of the breach; (3) the type of Personal Information obtained; and (4) telephonic contact information of the person whose system was breached. Notification is not required if it is determined that misuse of the information has not occurred and is not reasonably likely to occur.	Data shall not be considered to be encrypted if it is acquired in combination with any required key, security code, access code, or password that would permit access to the encrypted data.	Entities regulated by state or federal law that maintain procedures for addressing security breaches pursuant to those laws are exempt.	If engaged in trade or commerce, notify the regulator which has authority over such trade or commerce. All others notify AG. **Proposed Legislation H.B. 1613: Requires financial institutions to file a copy of reports relative to security breach notification with the bank commissioner.** Notice to other entities required. Waiver not permitted.	Up to $10,000 per violation. (NH RSA 358-A:4)	Person injured as a result of violation may bring an action for damages. Recovery may be in the amount of actual damages (two to three times actual damages if violation was knowing and willful). Injunctive relief permitted also.

MINTZ LEVIN

State and Bill Number	Data and consumers protected/Definition of Breach	Covered entities	Notice Procedures/ Timing/Exemptions	Encryption Safe Harbor	General & Preemption	Other provisions	Penalties	Private Cause of Action
New Jersey A 4001/S. 1914 N.J. Stat. 56:8-163 Proposed Legislation A.B. 175: Enhances duty and broadens liability in responses to security breach.	Personal information of New Jersey residents. Data elements alone may constitute "personal information" in certain situations. Security Breach: Unauthorized access to electronic files, media or data containing PI that compromises the security, confidentiality or integrity of PI when access to the PI has not been secured by encryption or by any other method of technology that renders the PI unreadable or unusable. Good-faith acquisition, release or use by employee or agent for purposes of entity is not breach if PI is not used or subject to further unauthorized disclosure	Any business that conducts business in New Jersey or any public entity that compiles or maintains computerized records that include personal information.	Written or electronic 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 means specified in the statute allowed in the case of very large breaches. Notice not required if the entity responsible for the data establishes that misuse of the information is not reasonably possible. Such determinations must be documented in writing and retained for five (5) years. An entity that must notify more than 1,000 persons at one time of a security breach is required to also promptly notify all consumer reporting agencies of the breach. **State Police must be notified before consumers are notified.**	Statute not applicable if the personal data that was lost, stolen, or accessed by an unauthorized individual is encrypted or secured by any other method or technology that renders the personal information unreadable or unusable.	Notice must be provided (in advance of notice to the consumer) to the Division of State Police in the Department of Law and Public Safety for investigation and handling. Notice to other entities is required.	Allows consumers to place a security freeze on their credit report.		No.

State and Bill Number	Data and consumers protected/Definition of Breach	Covered entities	Notice Procedures/ Timing/Exemptions	Encryption Safe Harbor	General & Preemption	Other provisions	Penalties	Private Cause of Action
New York A 4254,A 3492 N.Y. St. Tech. Law §208 (apply to state agencies) and Gen. Bus. Law, Sect. 899-aa (apply to business) N.Y. Gen. Bus. Law § 899-aa	"Personal information" = information concerning a natural person which, because of name, number, personal mark or other identifier can be used to identify such natural person. Private Information = personal information plus data elements of typical PI definition. Security Breach; Unauthorized acquisition or acquisition without valid authorization of computerized data that compromises the security, confidentiality or integrity of private information. Determination of whether private information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization can include factors such as: (a) Indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information (b) Indications that the information has been downloaded or copied(c) Indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of ID theft reported. Good-faith acquisition, release or use by employee or agent for purposes of entity is not breach if PI is not used	Any state entity that owns or licenses computerized data that includes private information and any person or business that conducts business in New York that owns or licenses computerized data containing private information.	**Specific notice content required.** State entities must provide written or electronic notice to affected persons within the most expedient time possible and without unreasonable delay, unless disclosure impedes law enforcement investigation. Notice must provide contact information for the person or business making the notification and a description of the categories of information that were, or are reasonably believed to have been acquired by another person without valid authorization, including specification of the elements of Personal information and private information which were, or are reasonably believed to have been, acquired. Breached entities must provide written, electronic or telephonic notice 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 means specified in the statute allowed in the case of very large breaches. In the event that notice of the security breach must be given to more than 5,000 persons at one time, the breached entity is required to also promptly notify all consumer reporting agencies of the breach.	Statute not applicable if the personal data that was lost, stolen, or accessed by an unauthorized individual is encrypted. No safe harbor if the compromised data was "encrypted with an encryption key that has also been acquired."		Electronic notice allowed only when the consumer to be notified has consented to such notice. A log of all consumers notified electronically must be kept. Notice to other entities required. **Notice must also be provided to the Attorney General, the State Consumer Protection Board and the Office of Cyber Security and Critical Infrastructure Coordination.** **Reporting form required**	Civil penalty of the greater of $5,000 or up to $10,000 per instance of failed notification, provided that the latter amount shall not exceed $150,000.	No. Attorney General may bring action on behalf of victims of a security breach. Two year statute of limitation.

State and Bill Number	Data and consumers protected/Definition of Breach	Covered entities	Notice Procedures/ Timing/Exemptions	Encryption Safe Harbor	General & Preemption	Other provisions	Penalties	Private Cause of Action
New York City N.Y. City Admin. Code §20-117	Personal Information of residents of the City of New York	Any business subject to the jurisdiction of the Department of Consumer Affairs that also owns, leases or maintains data that included Personal Information.	As soon as practicable, provided that the timing is not inconsistent with law enforcement or any other investigation or protective measures to restore the reasonably integrity of the system. Entities that maintain data must give notice to the owner of the data. Notice must be provided to the Department of Consumer Affairs and to the NYPD.	None. Applies to any breach of security, including non-electronic data.		Notice to other entities required.	Fine of not more than $400 and a person or entity that violates the law is liable for a civil penalty of $100 for each violation.	No.

MINTZ LEVIN

State and Bill Number	Data and consumers protected/Definition of Breach	Covered entities	Notice Procedures/ Timing/Exemptions	Encryption Safe Harbor	General & Preemption	Other provisions	Penalties	Private Cause of Action
North Carolina S.B. 1048 N.C. Gen'l Stat., ch. 75, §65	**Expanded definition of PI.** Personal information of North Carolina residents, including mother's maiden name, computer system password, electronic signature, or unique biometric data that is fingerprint, voice print, retinal image or iris image . Security Breach: An incident of unauthorized access to and acquisition of unencrypted and unredacted records or data containing PI where illegal use of the PI has occurred or is reasonably likely to occur or that creates a material risk of harm to a consumer Good-faith acquisition, release or use by employee or agent for purposes of entity is not breach if PI is not used or subject to further unauthorized disclosure	Any business that owns or licenses personal information of residents of North Carolina or any business that conducts business in North Carolina that owns or licenses personal information **in any form, whether computerized, paper, or otherwise.**	**Specific notice content required.** Written, electronic or telephonic notice 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 means specified in the statute allowed in the case of very large breaches. Notice not required if the entity responsible for the data concludes that the security breach is not reasonably likely to cause or create a "material risk of harm" to consumers. An entity that must notify more than 1,000 persons at one time of a security breach is required to also promptly notify all consumer reporting agencies of the breach.	Statute not applicable if the personal data that was lost, stolen, or accessed by an unauthorized individual is encrypted or redacted. No safe harbor if the compromised data is encrypted with an encryption key that has been acquired. "Encryption" defined as "the use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without use of a confidential process or key." "Redaction" defined as "the rendering of data so that it is unreadable or is truncated so that no more than the last four digits of the identification number is accessible as part of the data."	Financial institutions subject to and in compliance with the Federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice are exempt.	Gives affected consumers the right to place a security freeze on their credit reports. Notice to other entities required. Waiver not permitted **Must file North Carolina Security Breach Reporting Form**	Civil and criminal penalties for violations. Violation of this law is a violation of §75-1.1	Yes, but only if the individual is actually injured as a result of a violation of the statute.

State and Bill Number	Data and consumers protected/Definition of Breach	Covered entities	Notice Procedures/ Timing/Exemptions	Encryption Safe Harbor	General & Preemption	Other provisions	Penalties	Private Cause of Action
			Notice must include all of the following: (1) a description of the incident in general terms; (2) a description of the type of Personal Information subject to the breach; (3) a description of the general acts of the business to protect information from further breaches; (4) a telephone number for the business that a person may call for further information; (5) advice that directs the person to remain vigilant in reviewing account statements and monitoring free credit reports; 6) the toll-free numbers and addresses for the major consumer reporting agencies; and (7) the toll-free numbers, addresses, and website addresses for the Federal Trade Commission and the NC AG's office, along with a statement that the individual can obtain information from these sources about ID theft. **Notice must be provided to Consumer Protection Division of the AG's office of the nature of the breach, the numbers of consumers affected by the breach, steps taken to investigate the breach, steps taken to prevent a similar breach in the future, and information regarding the timing, distribution and content of the notice.**					

MINTZ LEVIN

State and Bill Number	Data and consumers protected/Definition of Breach	Covered entities	Notice Procedures/ Timing/Exemptions	Encryption Safe Harbor	General & Preemption	Other provisions	Penalties	Private Cause of Action
North Dakota S.B. 2251 N.D. Cent. Code, tit. 51, ch. 30	Personal information of North Dakota residents. Definition of "personal information" includes date of birth, **mother's maiden name, employee identification number, birth/death/marriage certificate, and electronic signature.** **Security Breach**: Unauthorized acquisition of computerized data when access to PI has not been secured by encryption or by any other method or technology that renders the electronic files, media, or databases unreadable or unusable. Good-faith acquisition, release or use by employee or agent for purposes of entity is not breach if PI is not used or subject to further unauthorized disclosure	Any person that conducts business in North Dakota and owns or licenses computerized data that includes personal information.	Written or electronic 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 means specified in the statute allowed in the case of very large breaches.	Statute not applicable if the personal data that was lost, stolen, or accessed by an unauthorized individual is encrypted or secured by any other method or technology that renders the personal information unreadable or unusable.	Financial institutions, trust companies, and credit unions subject to and in compliance with federal regulations are exempt.		Civil and criminal penalties (identity theft felonies).	No. Enforcement by Attorney General only.

State and Bill Number	Data and consumers protected/Definition of Breach	Covered entities	Notice Procedures/ Timing/Exemptions	Encryption Safe Harbor	General & Preemption	Other provisions	Penalties	Private Cause of Action
Ohio H.B. 104 Oh. Rev. Code, tit. XIII, ch. 1349, §19	Personal information of Ohio residents. "Personal information" defined as "any information that describes anything about a person or that indicates actions done by or to a person, or that indicates that a person possesses certain personal characteristics, and that contains, and can be retrieved from a system by, a name, identifying number, a symbol, or other identifier assigned to a person." Security Breach: Unauthorized access to and acquisition of computerized data that compromises the security or confidentiality of PI and that causes, reasonably believed to have caused, or reasonably is believed will cause a material risk of ID theft or fraud/	Any state agency or agency of a political subdivision that owns or licenses computerized data that includes personal information and any person that owns or licenses computerized data that includes personal information.	Written, electronic or telephonic notice must be provided to victims of a security breach **no later than 45 days following the discovery of the breach**, unless disclosure impedes law enforcement investigation. Substitute notice by means prescribed in the statute allowed for businesses with less than ten (10) employees when notification costs exceed $10,000. Notification required solely in the case of breaches that have caused or are reasonably likely to cause a material risk of identity theft or other fraud to an Ohio resident. In the event that an entity must notify more than 1,000 persons at one time of a security breach is required to also promptly notify all consumer reporting agencies of the breach.	Statute not applicable if the personal data that was lost, stolen, or accessed by an unauthorized individual is encrypted or redacted. "Encryption" defined as "the use of algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key." "Redacted" is defined as "altered or truncated so that no more than the last four digits of a social security number, driver's license number, state identification card number, account number, or credit or debit card number is accessible as part of the data."	Financial institutions, trust companies, and credit unions subject to and in compliance with federal regulations are exempt. Entities regulated by sections 1171 to 1179 of the "Social Security Act," chapter 531, 49 Stat. 620 (1935), 42 U.S.C. 1320d to 1320d-8, and any corresponding regulations in 45 C.F.R. Parts 160 and 164 are also exempt.	Licensor of personal data must also give notice to the owner of the data. Notice to other entities required. Disclosure may be made pursuant to any provisions of a contract entered into by a covered entity with another covered entity prior to the date of the security breach if that contract does not conflict with any provision of OH law and does not waive any provision of this section.	Civil penalty of up to $1,000 for each day of non-compliance with statute, up to $5,000 per day after 60 days, and up to, and up to $10,000 per day after 90 days.	No. Enforcement by Attorney General only.

MINTZ LEVIN

State and Bill Number	Data and consumers protected/Definition of Breach	Covered entities	Notice Procedures/ Timing/Exemptions	Encryption Safe Harbor	General & Preemption	Other provisions	Penalties	Private Cause of Action
Oklahoma HB 2357 Ok. Stat., Tit. 24, §§ 161 to 166 (effective November 2008)	Personal information of Oklahoma residents. The unredacted or unencrypted person's first name or initial and last name combined with: SSN; driver's license or state ID #; acct #, credit or debit card #, combined with any required info that allows access to account; or any other financial info. Personal information shall not include publicly available information that is lawfully made available to the general public from federal, state, or local public records Applies to paper records Security Breach: Unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of PI maintained as part of a database of PI regarding multiple individuals, or the covered entity reasonably believed has caused or will cause ID theft or other fraud. Good-faith acquisition, release or use by employee or agent for purposes of entity is not breach if PI is not used or subject to further unauthorized disclosure	An individual or entity that owns or licenses computerized information that includes Personal Information of Oklahoma residents must disclose any breach of the security of such a system to that person if that person's unencrypted or unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person and that access has caused or it is believed will cause identity theft or fraud.	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. Notice may be delayed if a law enforcement agency determines and advises the individual or entity that notice will impede a criminal or civil investigation or homeland or national security. Substitute notice - of email, conspicuous posting of the notice on the agency's website if maintained, notification to major statewide media - can be used if the cost of notice will exceed $50,000 or if the number of affected class to be notified exceeds 100,000 or if there is insufficient contact information to provide notice. Substitute notice must consist of any **two** of the following : (a) email notice (if email addresses are known); (b) conspicuous posting on website (if one is maintained); and (c) notification to major statewide media.	The disclosure of encrypted personal information must be disclosed if the information is acquired and accessed in unencrypted form during a security breach or if the breach was accomplished by someone with access to a encryption key and the individual or entity believes that such breach has or will cause identity theft or fraud.	A financial institution that complies with the notification requirements prescribed by the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice is deemed to be compliance with this law. An entity that complies with the notification requirements or procedures pursuant to the rules, regulations, procedures, or guidelines established by the primary or functional federal regulator of the entity shall be deemed to be in compliance with the law.	An entity that maintains data that includes personal information must notify the owner or licensee of the information of any breach of security as soon as practical if it is believed that personal information was accessed and acquired by an unauthorized person. An entity that maintains its own notification procedures as part of an information privacy or security policy for the treatment of information that is consistent with the timing requirements of this law is deemed to be in compliance with the notification requirements of the law if it provides notice in a manner consistent with the law in the event of a security breach.	Actual damages resulting from a violation of the act or a civil penalty not to exceed $150,000 per breach of the security of the systems or series of breaches of a similar nature that are discovered in a single investigation. Violations of the act by state chartered or state licensed financial institutions may only be enforced by the primary state regulator of the institution.	No. Violations may be enforced by the Attorney General or a district attorney as an unlawful practice under the Oklahoma Consumer Protection Act.

MINTZ LEVIN

State and Bill Number	Data and consumers protected/Definition of Breach	Covered entities	Notice Procedures/ Timing/Exemptions	Encryption Safe Harbor	General & Preemption	Other provisions	Penalties	Private Cause of Action
Oregon Oregon Rev. Stat. § 646A.600 et seq.	Personal information of Oregon consumers. Personal information is defined as first name or initial and last name combined with one of the following: SSN, driver's license, state i.d. card number, passport, financial account information along with password or security code information. PI also includes any PI data element or any combination of the PI data elements if the information would be sufficient to permit an individual to fraudulently assume the identity of the OR resident whose information was compromised. Security Breach: Unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of PI Good-faith acquisition, release or use by employee or agent for purposes of entity is not breach if PI is not used or subject to further unauthorized disclosure	Any person that owns, maintains or otherwise possesses data that includes personal information that is used in the course of the person's business, vocation, occupation or volunteer activities.	Notice must be given in the most expeditious time possible and without unreasonable delay. Notice may be written, electronic or by telephone. Substitute notice can be used if the cost of notice will exceed $250,000 or if the number of consumers to be notified exceeds 350,000 or if there is insufficient contact information to provide notice. Notice not required if after investigation or consultation with relevant authorities, it is determined that no reasonable likelihood of harm will result. Minimum notice content requirements: (a) description of incident in general terms, (b) approximate date of security breach, (c) type of PI obtained as a result of the breach; (d) contact information of person; (e) contact information for national CRAs and (e) advice to individual to report suspected ID theft to law enforcement	Notification required if the data elements are encrypted but the encryption key has also been acquired.	Does not apply if covered entity complies with state or federal laws that provide greater protection and those subject to Title V of the GLBA.	Contains restrictions on including social security numbers in documents. Covered entities must "develop, implement and maintain" reasonable safeguards to protect personal information. Notice to other entities required.	$1,000 per violation. In the case of a continuing violation, each day's continuance is a separate violation. Maximum penalty of $500,000.	Compensation can be ordered by the state upon a finding that enforcement of the rights of consumers by private civil action would be so burdensome or expensive as to be impractical.

MINTZ LEVIN

State and Bill Number	Data and consumers protected/Definition of Breach	Covered entities	Notice Procedures/ Timing/Exemptions	Encryption Safe Harbor	General & Preemption	Other provisions	Penalties	Private Cause of Action
Pennsylvania S.B. 712 Pa. Cons. St., Tit. 73, ch. 43 §2301 - 2308	Personal information of Pennsylvania residents. Security Breach: Unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of PI maintained by the entity as part of a database of PI regarding multiple individuals and that causes or the entity reasonably believes has caused or will cause loss or injury to any resident of PA. Good faith acquisition by an employee or agent for purposes of the entity is not a breach if the PI is not used for a purpose other than the lawful purpose of the entity and is not subject to further unlawful disclosure.	Any entity that maintains, stores, or manages computerized data that contains personal information of Pennsylvania residents.	Written, telephonic or e-mail notice (only if a prior business relationship exists) must be provided to affected persons within the most expedient time possible and without unreasonable delay, unless disclosure impedes law enforcement investigation. Substitute notice by means prescribed in the statute allowed in the case of large breaches. Notice not required if the entity responsible for the data concludes that the breach did not materially compromise the personal information. In the event that the breached entity must notify more than 1,000 persons at one time of a security breach is required to also promptly notify all consumer reporting agencies of the breach.	Statute not applicable if the personal data that was lost, stolen, or accessed by an unauthorized individual is encrypted or redacted. "Encryption" defined as "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key." "Redacted" is defined as altered or truncated so that no more than the last four digits of a social security number, driver's license number, state identification card number, account number, or financial account number is accessible as part of the data.	Exception: Entity that maintains its own notification procedures are part of an information privacy or security policy for the treatment of PI and is consistent with the notice requirements if it notifies persons in accordance with its policies. Financial institutions subject to and in compliance with federal regulations are exempt. Entities that are in compliance with notification requirements and procedures established by the entities' primary or functional federal regulator are also exempt.	Notice of the breach must be provided if encrypted personal information is accessed and acquired in unencrypted form using the encryption key. Proposed legislation H.B. 2847: Requires disclosure to customers of any security of computerized records S.B. 155: Further provides for notification of breach.	Violation of the statute constitutes an unfair or deceptive act in violation of the Unfair Trade Practices and Consumer Protection Law.	No. Attorney General has exclusive authority to bring an action under the Unfair Trade Practices and Consumer Protection Law.

State and Bill Number	Data and consumers protected/Definition of Breach	Covered entities	Notice Procedures/ Timing/Exemptions	Encryption Safe Harbor	General & Preemption	Other provisions	Penalties	Private Cause of Action
Rhode Island H. 6191 R.I. Gen'l Law, tit. 11, ch. 49.2, §§1 thru 7	Personal information of Rhode Island residents. Definition of "personal information" includes physical characteristics, signature, address, telephone number, insurance policy number, education, employment, and employment history. Security Breach: Unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of PI. Good faith acquisition exception provided that the PI is not used or subject to further unauthorized disclosure	Any person or business that conducts business in Rhode Island and that owns or licenses computerized data that includes personal information.	Written or electronic 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 means prescribed in the statute allowed when the number of affected consumers exceeds $50,000 and notification costs exceed $25,000. Notice not required if law enforcement concludes that there is "no significant risk of identity theft."	Statute not applicable if the personal data that was lost, stolen, or accessed by an unauthorized individual is encrypted.	Entities subject to and in compliance with state and federal laws that provides greater protection to personal information and HIPAA are exempt. Exception for entities that maintain own security breach procedures as part of an information security policy and otherwise complies with the timing requirements of the statute deemed in compliance, provided notice is made in accordance with the policies. No waiver by contract or other means.	Businesses are required to implement reasonable data destruction and information security procedures.	Civil penalty of up to $100 per occurrence and not more than $25,000.	Yes. Plaintiff may also recover attorney fees and costs.

MINTZ LEVIN

State and Bill Number	Data and consumers protected/Definition of Breach	Covered entities	Notice Procedures/ Timing/Exemptions	Encryption Safe Harbor	General & Preemption	Other provisions	Penalties	Private Cause of Action
South Carolina S.B. 453 S.C. Code Ann. §39-1-90	Personal identifying information of individuals residing in South Carolina who undertake transactions for personal, family, or household purposes. Includes information issued by a governmental or regulatory entity that uniquely will identify an individual. Security Breach: Unauthorized access to and acquisition of computerized records or data that was not rendered unusable through encryption, redaction, or other methods, 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 a resident. Exemption for good-faith acquisition by an employee for the purposes of its business if the PI is not used or subject to further unauthorized disclosure.	A person conducting business in South Carolina, and owning or licensing computerized data or other data that includes personal identifying information. Consumer reporting agencies.	A person conducting business in South Carolina must notify the owner of data that is breached immediately upon discovery of the breach. May be delayed if a law enforcement agency determines that notice will compromise investigation. A consumer reporting agency, not later than the tenth business day after the date the agency receives the request for a security freeze shall send a written confirmation of the security freeze to the consumer and provide the consumer with a unique personal identification number or password to be used by the consumer to authorize a removal or temporary lifting of the security freeze. Notice must be written or electronic, if the entity's the person's primary method of communication with the individual is by electronic means. Substitute notice by means prescribed in the statute allowed in the case of very large breaches. If the entity provides notice to more than one thousand persons at one time notice must be given to the Consumer Protection Division of the Department of Consumer Affairs and the consumer reporting agencies.	Statute applies only to unencrypted personal data in both paper and electronic forms accessed by an unauthorized person for an unlawful purpose.	Financial institutions as defined in Title V of the GLBA, health insurers subject to HIPAA, persons complying with a court order, and consumer reporting agencies in compliance with the Fair Credit Reporting Act are exempt.	A person that maintains its own notification procedures as part of an information security policy for the treatment of personal identifying information and is otherwise consistent with the timing requirements of this section is considered to be in compliance with the notification requirements of this section if the person notifies subject persons in accordance with its policies in the event of a breach of security of the system.	Three times the amount of actual damages or not more than one thousand dollars for each incident, whichever is greater, as well as reasonable attorneys' fees and costs. If a credit reporting agency fails to impose a freeze after being notified of a breach, then damages may be increased by one thousand dollars each day until the security freeze is imposed.	A resident of South Carolina who is injured by a violation of this section, in addition to and cumulative of all other rights and remedies available at law, may institute a civil action to recover damages and recover attorneys' fees and costs if successful.

MINTZ LEVIN

State and Bill Number	Data and consumers protected/Definition of Breach	Covered entities	Notice Procedures/ Timing/Exemptions	Encryption Safe Harbor	General & Preemption	Other provisions	Penalties	Private Cause of Action
Tennessee S.B. 2220 Tenn. Code, tit. 47, ch. 18, §§2101-2107	Personal information of Tennessee residents. Security Breach: Unauthorized acquisition of unencrypted computerized data that materially compromises the security, confidentiality or integrity of PI. Good faith exception provided that the PI is not used or subject to further unauthorized disclosure.	Any person or business that conducts business in Tennessee, or any agency of the state of Tennessee or any of its political subdivisions, that owns or licenses computerized data that includes personal information.	Written or electronic 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 or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. Substitute notice by means prescribed in the statute allowed in the case of very large breaches. If an entity is required to notify more than 1,000 persons at one time, must report to all CRAs and credit bureaus that compile and maintain files on consumers of the timing, distribution and content of the notices.	Statute not applicable if the personal data that was lost, stolen, or accessed by an unauthorized individual is encrypted.	Entities subject to Title V of the GLBA are exempt. Exception for entities that maintain own notification procedures as part of an information security policy that is otherwise consistent with the notification requirements of the statute if it notifies subject persons in accordance with such policies.	Businesses must have reasonable data destruction security procedures.	Residents injured by a violation may recover damages, as well as injunctive relief, to enjoin from further actions in violation of law.	Yes.

State and Bill Number	Data and consumers protected/Definition of Breach	Covered entities	Notice Procedures/ Timing/Exemptions	Encryption Safe Harbor	General & Preemption	Other provisions	Penalties	Private Cause of Action
Texas S.B. 122 Tex. Bus. & Com. Code § 521.03 Amended by H.B. 2004, eff. Sept. 1, 2009 Amendment: HB 300, effective Sept. 1, 2012	Personal information of Texas residents. Definition of "personal information" includes date of birth, mother's maiden name, telecommunication access device and unique biometric data, health and medical information including information regarding physical or mental condition, provision of health care, or payment for health care. Security Breach: Unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of sensitive PI, **including data that is encrypted if the person accessing the data has the key to decrypt the data.** Exception for good faith acquisition of PI.	Any person that conducts business in Texas and owns or licenses computerized data that includes sensitive personal information. Requires public agencies to notify state residents if their PI is breached.	Written or electronic 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 or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system. Substitute notice by means prescribed in the statute allowed in the case of very large breaches of 500,000 people or the cost of notification exceeds $250,000. In the event that the breached entity must notify more than 10,000 persons at one time of a security breach is required to also promptly notify all consumer reporting agencies of the breach. Amendment effective 9/1/2012: Specifically requires notification of data breaches to residents of states that have not enacted their own law requiring such notification	Statute not applicable if the personal data that was lost, stolen, or accessed by an unauthorized individual is encrypted, EXCEPT in the event that the encryption key is also breached.	Entities subject to Title V of the GLBA are exempt.	Businesses required to have data destruction security procedures.	Civil penalty of at least $2,000 but not more than $50,000 for each violation. (Effective 9.1.2012 – increases to $100 per individual per day of failed or delayed notification, not to exceed $250,000 for a single breach) **Effective 9.1.2012 under HB300: any business failing to make required breach notifications for breaches of protected health information – penalties of up to $250,000 for a single breach** **Any individual who accesses, reads, scans, stores or transfers protected health information electronically and without authorized may be charged with a felony**	No. Enforcement by Attorney General only.

State and Bill Number	Data and consumers protected/Definition of Breach	Covered entities	Notice Procedures/ Timing/Exemptions	Encryption Safe Harbor	General & Preemption	Other provisions	Penalties	Private Cause of Action
Utah S.B. 69 Utah Code §§ 13-44-101, -102, -201, -202, -301	Personal information of Utah residents.	Any person who owns or licenses computerized data that includes personal information concerning a Utah resident.	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. Notice of the security breach may also be provided via publication in a newspaper of general circulation.	Statute not applicable if the personal data that was lost, stolen, or accessed by an unauthorized individual is encrypted or protected by another method that renders the data unreadable or unusable.	Entities regulated by state or federal law that maintain procedures for addressing security breaches pursuant to those laws are exempt.	All entities that conduct business in the state are required to maintain reasonable data protection measures.	Fine no greater than $2,500 per violation or series of violations concerning a specific consumer, and no greater than $100,000 in the aggregate for related violations concerning more than one consumer.	No. Enforcement by Attorney General only.
Vermont SB 284 Vermont. Stat., tit. 9 §§2430-2445	Personal information of Vermont residents. Person's first name or initial and last name combined with: SSN; driver's license or state ID #; acct #, credit or debit card #, combined with any required info that allows access to account; or any other financial info. Also includes acct #s on their own and passwords, pin #s on their own. Does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records	State agency, university, corporation, LLC, financial institution, retail operator or other retail entity that handles, collects disseminates or otherwise deals with nonpublic personal information.	Notice only required if misuse is not reasonably possible and provides notice that misuse is not possible. Allows telephonic notice of breach. Substitute notice allowed when cost of providing notice would exceed $50,000 or affected class of individuals to be notified exceeds 5,000. If more than 1,000 persons must be notified at one time, CRA must also be notified.	Excludes info redacted or not protected by another method that renders the data unreadable or unusable.	Financial institutions subject to certain federal interagency guidance regarding consumer information are exempt.	H.B. 474 and S.B. 149:: Propose to repeal the sunset of the exemption for law enforcement agencies from the security breach notice act Proposed Legislation H.B. 722: Proposed revisions to notification laws.	Up to $10,000 per violation.	Attorney General and State Attorney have enforcement power, Individuals have a right to seek an injunction.

Current as of October 1, 2011 – FOR INFORMATIONAL PURPOSES ONLY

MINTZ LEVIN

State and Bill Number	Data and consumers protected/Definition of Breach	Covered entities	Notice Procedures/ Timing/Exemptions	Encryption Safe Harbor	General & Preemption	Other provisions	Penalties	Private Cause of Action
Virginia SB 307.2 Virginia Code § 18.2-186.6	Personal information of Virginia residents.	Any individual or entity storing personal information of Virginia residents. Entity includes corporations, business trusts, estates, partnerships, limited partnerships, limited liability partnerships, limited liability companies, associations, organizations, joint ventures, governments, governmental subdivisions, agencies, or instrumentalities or any other legal entity, whether for profit or not for profit.	Individuals and entities must disclose any breach of the security of the system following discovery or notification of the breach of the security of the system to the Office of the Attorney General and any affected Virginia resident. Notice may be written, telephonic, or electronic. Substitute notice by means prescribed in the statute allowed in the case of very large breaches. Notice must include a description of the incident in general terms, the type of personal information that was breached, the general acts of the individual or entity to protect the personal information from further breaches, a telephone number that the person may call for further information and assistance, and advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports. In the event an individual or entity provides notice to more than 1,000 persons at one time pursuant to this section, the individual or entity shall notify, without unreasonable delay, the Office of the Attorney General and the consumer reporting agencies.	Statute applies only to unencrypted and unredacted computerized data that the owner of the data reasonably believes will result in identity theft or other fraud. "Encrypted" means the transformation of data through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without the use of a confidential process or key, or the securing of the information by another method that renders the data elements unreadable or unusable. "Redact" means alteration or truncation of data such that no more than the following are accessible as part of the personal information.	An entity that maintains its own notification procedures as part of an information privacy or security policy that is consistent with the statute, an entity that is subject to Title V of the GLBA , or an entity that complies with the notification requirements of the entity's primary state or federal regulator.	Statute permits notice of the breach to be given via telephone, e-mail, or in writing.	Attorney General may bring an action and may impose a civil penalty not to exceed $150,000 per breach of the security of the system or a series of breaches of a similar nature that are discovered in a single investigation.	Yes.

State and Bill Number	Data and consumers protected/Definition of Breach	Covered entities	Notice Procedures/ Timing/Exemptions	Encryption Safe Harbor	General & Preemption	Other provisions	Penalties	Private Cause of Action
Washington S.B. 6043 Wa. Rev. Code, tit. 19, §255.010; Amended by H.B. 1149 (Effective July 1, 2010).	Personal information of Washington residents.	Any person or business that conducts business in Washington and owns or licenses computerized data that includes personal information; as well as any agency that owns or licenses computerized data that includes personal information. Any business or credit card processor that fails to comply with PCI security standards and subsequently experiences a breach	Written or electronic 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 means prescribed in the statute allowed in the case of very large breaches. Notice not required in the case of a technical breach of the security system which does not reasonably subject consumers to a "risk of criminal activity."	Statute not applicable if the personal data that was lost, stolen, or accessed by an unauthorized individual is encrypted.		If a processor or business fails to take reasonable care to guard against unauthorized access to account information that is in the possession or under the control of the business or processor, and the failure is found to be the proximate cause of a breach, the processor or business is liable to a financial institution for reimbursement of reasonable actual costs related to the reissuance of credit cards and debit cards that are incurred by the financial institution to mitigate potential current or future damages to its credit card and debit card holders that reside in the state of Washington	Civil liabilities imposed for damages caused by failure to comply with the statute. Any business that violates this statute may be enjoined. Waivers of this statute are unenforceable.	Yes.

State and Bill Number	Data and consumers protected/Definition of Breach	Covered entities	Notice Procedures/ Timing/Exemptions	Encryption Safe Harbor	General & Preemption	Other provisions	Penalties	Private Cause of Action
West Virginia S.B. 340 W.V. Code § 46A-2A-101	Personal information of West Virginia residents.	An individual or entity that owns or licenses computerized data that includes personal information. Entity includes corporations, business trusts, estates, partnerships, limited partnerships, limited liability partnerships, limited liability companies, associations, organizations, joint ventures, governments, governmental subdivisions, agencies, or instrumentalities or any other legal entity, whether for profit or not for profit.	Individual or entity must give notice if encrypted information is accessed and acquired in an unencrypted form or if the security breach involves a person with access to the encryption key and the individual or entity reasonably believes that such breach has caused or will cause identity theft or other fraud to any resident of West Virginia. Notice may be written, telephonic, or electronic. Substitute notice by means prescribed in the statute allowed in the case of very large breaches. Notice shall include a description of the categories of information breached, a telephone number or website address that the individual may use to contact the entity or the agent of the entity and from whom the individual may learn what types of information the entity maintained about that individual or about individuals in general, whether the entity maintained information about that individual, and the toll-free contact telephone numbers and addresses for the major credit reporting agencies and information on how to place a fraud alert or security freeze.	Statute applies only to unencrypted and unredacted computerized data that the owner of the data reasonably believes will result in identity theft or other fraud. “Encrypted" means transformation of data through the use of an algorithmic process to into a form in which there is a low probability of assigning meaning without use of a confidential process or key or securing the information by another method that renders the data elements unreadable or unusable. "Redact" means alteration or truncation of data such that no more than the last four digits of a social security number, driver's license number, state identification card number or account number is accessible as part of the personal information.	An entity that maintains its own notification procedures as part of an information privacy or security policy that is consistent with the statute, an entity that is subject to Title V of the GLBA, or an entity that complies with the notification requirements of the entity's primary state or federal regulator.		Attorney General has exclusive authority to bring action. No civil penalty may be assessed unless the court finds that the defendant has engaged in a course of repeated and willful violations. No civil penalty shall exceed one hundred fifty thousand dollars per breach or series of breaches of a similar nature that are discovered in a single investigation.	No.

MINTZ LEVIN

State and Bill Number	Data and consumers protected/Definition of Breach	Covered entities	Notice Procedures/ Timing/Exemptions	Encryption Safe Harbor	General & Preemption	Other provisions	Penalties	Private Cause of Action
Wisconsin S.B. 164 Wisc. Stat., ch. 895, §507 Wis. Stat. § 134.98 et seq.	Personal information of Wisconsin residents. PI means an individual's first name or initial and last name combined with: SSN; driver's license or state ID #; acct #, credit or debit card #, combined with any required info that allows access to account or any other financial info, biometric data and the individual's deoxyribonucleic acid profile. If information is publicly available information, then it is not covered.	All entities, including state and local governments that engage in one of the following activities: (i) conduct business in Wisconsin and maintain personal information in the ordinary course of business; (ii) license personal information in Wisconsin; (iii) maintain a depository account for a Wisconsin resident; or (iv) lend money to a Wisconsin resident.	If it is entity whose principal place of business is located in this state or an entity that maintains or licenses personal information in this state, the entity shall make reasonable efforts to notify each subject of the personal information. The notice shall indicate that the entity knows of the unauthorized acquisition of personal information pertaining to the subject of the personal information. If an entity whose principal place of business is not located in this state, the entity shall make reasonable efforts to notify each resident of this state who is the subject of the personal information. The notice shall indicate that the entity knows of the unauthorized acquisition of personal information pertaining to the resident of this state who is the subject of the personal information. Notice must be provided to victims of a security breach, by mail or a method previously used to communicate with the affected individuals, within a reasonable time, not to exceed 45 days, unless disclosure impedes law enforcement investigation. Substitute notice by means prescribed in the statute allowed when the mailing address of the affected individual(s) is unknown. Notice 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. In the event that an entity must notify more than 1,000 or more persons at one	Statute not applicable if the personal data that was lost, stolen, or accessed by an unauthorized individual is encrypted redacted or altered in a manner that renders it unreadable.	Entities regulated by certain federal law mentioned in section 3(m) of the statute are exempt.			

State and Bill Number	Data and consumers protected/Definition of Breach	Covered entities	Notice Procedures/ Timing/Exemptions	Encryption Safe Harbor	General & Preemption	Other provisions	Penalties	Private Cause of Action
Wyoming H.B. 208 S.B. 194 Wyo.Stat. 40-12-501-509	Personal identifying information about a resident of Wyoming.	Any individual or commercial entity that conducts business in Wyoming and that owns or licenses computerized data that includes personal identifying information about a resident of Wyoming.	An individual or entity, when it becomes aware of a breach of the security of the system, must conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal identifying information has been or will be misused. If the investigation determines that the misuse of personal identifying information about a Wyoming resident has occurred or is reasonably likely to occur, the individual or the commercial entity shall give notice as soon as possible to the affected Wyoming resident. Notice may be written or electronic. Substitute notice by means prescribed in the statute allowed in the case of very large breaches. Notice must include a toll-free number that the individual may use to contact the person collecting the data and the toll-free contact telephone numbers and addresses for the major credit reporting agencies.	None.	Entities subject to and in compliance with the privacy and security provisions of Title V of the GLBA are exempt.		A civil penalty of $1,000 for a consumer reporting agency's failure to comply with notification requirements.	A consumer may file a complaint with the federal trade commission and the state attorney general. If a consumer reporting agency intentionally or negligently violates a valid security freeze, the consumer may bring a civil action to recover damages, including attorneys' fees and costs.

State and Bill Number	Data and consumers protected/Definition of Breach	Covered entities	Notice Procedures/ Timing/Exemptions	Encryption Safe Harbor	General & Preemption	Other provisions	Penalties	Private Cause of Action
District of Columbia* Bill 16-810 D.C. Code § 28-3851, 3852, 3853	Personal information stored in computerized or other electronic form. Statute is not limited to D.C. residents.	Any person or entity who conducts business in the District of Columbia, and who, in the course of such business, owns or licenses computerized or other electronic data that includes personal information.	Upon discovery of breach, person or entity must promptly notify any District of Columbia resident whose personal information was included in the breach, in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement. This applies even if the person or entity that discovers the breach does not own the compromised data. If the breach involves personal information of more than 1,000 people, the person or entity must also notify consumer reporting agencies. Notice must be written or electronic, if the customer has consented to receipt of electronic notice. Substitute notice by means prescribed in the statute allowed in the case of very large breaches.	None.	Entities subject to Title V of the GLBA are exempt.		Attorney General may bring petition for temporary or permanent injunctive relief and for an award of restitution for property lost or damages suffered by D.C. residents. Attorney General may recover a civil penalty not to exceed $100 for each violation, the costs of the action, and reasonable attorney's fees. Each failure to provide a D.C. resident with notification is a separate violation.	Yes. Any D.C. resident may bring a civil action to recover actual damages, the costs of the action, and reasonable attorney's fees. Actual damages shall not include dignitary damages, including pain and suffering.

State and Bill Number	Data and consumers protected/Definition of Breach	Covered entities	Notice Procedures/ Timing/Exemptions	Encryption Safe Harbor	General & Preemption	Other provisions	Penalties	Private Cause of Action
Puerto Rico* Bill 111 10 Laws of Puerto Rico Tit. 10. Subtit. 3. Ch. 310 § 4051 et. seq.	Personal information of Puerto Rico residents. At least the name or first initial and the surname of a person, together with the persons (1) SSN (2) driver's license #, voter identification # or other official identification #(3) Bank or financial account numbers of any type with or without passwords or code access (4) Names of users and passwords or access codes to public or private information systems (5) Medical information protected by HIPAA (6) Tax info (7) Work related evaluation (8) Lab results Neither the mailing nor the residential address is included in the protected information or information that is a public document and that is available to the citizens in general. Security Breach: Unauthorized access to storage of PI that compromises the security, confidentiality or integrity of the PI or access by persons who are authorized who have knowingly violated confidentiality obligations. Includes access to PI through computer system as well as physical access.	Any entity that is the proprietor or custodian of a data bank for commercial use that includes personal information of citizens who reside in Puerto Rico.	Clients must be notified as expeditiously as possible, taking into consideration the need of law enforcement agencies to secure possible crime scenes and evidence as well as the application of measures needed to restore the system's security. Within a non-extendable term of ten (10) days after the violation of the system's security has been detected, the parties responsible shall inform the Department of Consumer Affairs, which shall make a public announcement of the fact within twenty-four (24) hours after having received the information. Notice must be written or electronic. Substitute notice by means prescribed in the statute allowed in the case of very large breaches.	Yes. Statute applies to data that is not protected by a cryptographic code but only by a password.		No provision of this chapter is prejudicial to those institutional information and security policies that an enterprise or entity may have in force to provide protection equal or better to the protection called for by the statute.	Fines of $500 up to a maximum of $5000 for each violation.	Yes. Consumers may bring actions apart from the statute.

Current as of October 1, 2011 – FOR INFORMATIONAL PURPOSES ONLY

State and Bill Number	Data and consumers protected/Definition of Breach	Covered entities	Notice Procedures/ Timing/Exemptions	Encryption Safe Harbor	General & Preemption	Other provisions	Penalties	Private Cause of Action
Virgin Islands* Bill 6789 14 V.I. Code Ch. 110. Sub. Ch. I § 2208 - 2209	Personal information of Virgin Islands residents. PI means an individual's first name or initial and last name combined with: SSN; driver's license or state ID #; acct #, credit or debit card #, combined with any required info that allows access to account or any other financial info, If information is publicly available information, then it is not covered.	Any person or business that conducts business in the Virgin Islands, and that owns or licenses computerized data that includes personal information.	Upon discovery of breach, disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement. Notice must be written or electronic. Substitute notice by means prescribed in the statute allowed in the case of very large breaches.	Yes.		Any waiver of the provisions of the statute is contrary to public policy, and is void and unenforceable.	Any business that violates, proposes to violate, or has violated this title may be enjoined. Statute does not contain fines.	Yes. Any customer injured by a violation of this title may commence a civil action to recover damages.

Current as of October 1, 2011 – FOR INFORMATIONAL PURPOSES ONLY