Revised June 2016

PERKINSCOIE
COUNSEL TO GREAT COMPANIES

Security Breach Notification Chart

Perkins Coie's Privacy & Security practice maintains this comprehensive chart of state laws regarding security breach notification. The chart is for informational purposes only and is intended as an aid in understanding each state's sometimes unique security breach notification requirements. Lawyers, compliance professionals, and business owners have told us that the chart has been helpful when preparing for and responding to data breaches. We hope that you find it useful as well.

Alabama*
Alaska
Arizona
Arkansas
California
Colorado
Connecticut
Delaware
District of Columbia
Florida
Georgia
Hawaii
Idaho
Illinois
Indiana
Iowa
Kansas
Kentucky
Louisiana
Maine
Maryland
Massachusetts
Michigan
Minnesota
Mississippi
Missouri
Montana
Nebraska
Nevada
New Hampshire
New Jersey
New Mexico*
New York
North Carolina
North Dakota
Ohio
Oklahoma
Oregon
Pennsylvania
Puerto Rico
Rhode Island
South Carolina
South Dakota*
Tennessee
Texas
Utah
Vermont
Virginia
Washington
West Virginia
Wisconsin
Wyoming

* No legislation specifically pertaining to security breach notification. For entities doing business in Texas, see Texas law.

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

Alaska

Alaska Stat. § 45.48.010 *et seq*.

H.B. 65 (signed into law June 13, 2008, Chapter 92 SLA 08)

Effective July 1, 2009

[back to table of contents]

Application. Any person, state, or local governmental agency (excepting the judicial branch), or person with more than 10 employees (collectively, Entity) that owns or licenses PI in any form in AK that includes PI of an AK resident.

- The provisions governing maintenance of PI that the Entity does not own appear applicable to any Entity maintaining information on state residents, whether or not the Entity conducts business in AK.

Security Breach Definition. An unauthorized acquisition or reasonable belief of unauthorized acquisition of PI that compromises the security, confidentiality, or integrity of the PI maintained by the Entity. Acquisition includes acquisition by photocopying, facsimile, or other paper-based method; a device, including a computer, that can read, write, or store information that is represented in numerical form; or a method not identified in this paragraph.

- Good-faith acquisition of PI by an employee or agent of the Entity for a legitimate purpose of the Entity is not a breach of the security of the information system if the employee or agent does not use the PI for a purpose unrelated to a legitimate purpose of the Entity and does not make further unauthorized disclosure of the PI.

Notification Obligation. Any Entity to which the statute applies shall disclose the breach to each AK resident whose PI was subject to the breach after discovering or being notified of the breach.

- Notification is not required if, after an appropriate investigation and after written notification to the state AG, the Entity determines that there is not a reasonable likelihood that harm to the consumers whose PI has been acquired has resulted or will result from the breach. The determination shall be documented in writing and the documentation shall be maintained for five years.

Notification of Consumer Reporting Agencies. If an Entity is required to notify more than 1,000 AK residents of a breach, the Entity shall also notify without unreasonable delay all consumer credit reporting agencies that compile and maintain files on consumers on a nationwide basis and provide the agencies with the timing, distribution, and content of the notices to AK residents. Entities subject to the Gramm-Leach-Bliley Act are exempt from this requirement and are not required to notify consumer reporting agencies.

Third-Party Data Notification. If a breach of the security of the information system containing PI on an AK resident that is maintained by an Entity that does not own or have the right to license the PI occurs, the Entity shall notify the Entity that owns or licensed the use of the PI about the breach and cooperate as necessary to allow the Entity that owns or licensed the use of the PI to comply with the statute.

Timing of Notification. The disclosure shall be made in the most expeditious time possible and without unreasonable delay consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the information system.

Personal Information Definition. Information in any form on an individual that is not encrypted or redacted, or is encrypted and the encryption key has been accessed or acquired, and that consists of a combination of an individual's first name or first initial and last name in combination with any one

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	or more of the following data elements: • Social Security Number; • Driver license number or state identification card number; or • Account number or credit card number or debit card number, except if these can only be accessed with a personal code, then the account, credit card, or debit card number in combination with any required security code, access code, or password. • Passwords, personal identification numbers, or other access codes for financial accounts **Notice Required.** Notice may be provided by one of the following methods: • Written notice; • Telephonic notice; or • Electronic notice if the Entity's primary method of communication with the AK resident is by electronic means or is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 (E-SIGN Act). Disclosure is not required if, after an appropriate investigation and after written notification to the attorney general, the Entity determines that there is not a reasonable likelihood that harm to the consumers whose personal information has been acquired has resulted or will result from the breach. The determination shall be documented in writing, and the documentation shall be maintained for five years. The notification required may not be considered a public record open to inspection by the public**.** **Substitute Notice Available.** If the Entity can demonstrate that the cost of providing notice will exceed $150,000,that the affected class of persons to be notified exceeds 300,000, or that the Entity does not have sufficient contact information to provide notice. Substitute notice shall consist of <u>all</u> of the following: • Email notice if the Entity has email addresses for the state resident subject to the notice; • Conspicuous posting of the notice on the Web site of the Entity if the Entity maintains one; and • Notification to major statewide media. **Penalties.** • An Entity that is a governmental agency is liable to the state for a civil penalty of up to $500 for each state resident who was not notified (the total penalty may not exceed $50,000) and may be enjoined from further violations. • An Entity that is not a governmental agency is liable to the state for a civil penalty of up to $500 for each state resident who was not notified (the total civil penalty may not exceed $50,000). **Other Key Provisions:** • **Delay for Law Enforcement.** Notice may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation. Notice required by the statute must be

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	made after the law enforcement agency determines that notification will no longer impede the investigation. • **Private Right of Action.** A person injured by a breach may bring an action against a non-governmental Entity. • **Waiver Not Permitted.**

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

Arizona

Ariz. Rev. Stat. § 44-7501

S.B. 1338 (signed into law April 26, 2006, Chapter 232)

Effective December 31, 2006

[back to table of contents]

Application. Any person or entity (collectively, Entity) that conducts business in AZ and that owns or licenses unencrypted computerized data that includes PI.

- The provisions governing maintenance of PI that the Entity does not own appear applicable to any Entity maintaining information on state residents, whether or not the Entity conducts business in the state.

Security Breach Definition. An unauthorized acquisition of and access to unencrypted or unredacted computerized data that materially compromises the security or confidentiality of PI maintained by an Entity as part of a database of PI regarding multiple individuals and that causes or is reasonably likely to cause substantial economic loss to an individual.

- Good-faith acquisition of PI by an employee or agent of the Entity for the purposes of the Entity is not a breach of the security system if the PI is not used for a purpose unrelated to the Entity or subject to further willful unauthorized disclosure.

Notification Obligation. Any Entity to which the statute applies shall notify the individuals affected when it becomes aware of an incident of unauthorized acquisition and access to unencrypted or unredacted computerized data that includes an individual's PI.

- An Entity is not required to disclose a breach of the system if the Entity or a law enforcement agency, after a reasonable investigation, determines that a breach of the security of the system has not occurred or is not reasonably likely to occur.

Third-Party Data Notification. If an Entity maintains unencrypted data that includes PI that the Entity does not own, the Entity shall notify and cooperate with the owner or the licensee of the information of any breach of the security of the system following discovery of the breach without unreasonable delay. Cooperation shall include sharing information relevant to the breach of the security of the system with the owner or licensee. The person or entity that owns or licenses the computerized data shall provide notice to the individual. The Entity that maintained the data under an agreement with the owner or licensee is not required to provide notice to the individual unless the agreement stipulates otherwise.

Timing of Notification. The disclosure shall be made in the most expedient manner possible and without unreasonable delay consistent with any measures necessary to determine the nature and scope of the breach, to identify the individual affected or to restore the reasonable integrity of the data system.

Personal Information Definition. An individual's first name or first initial and last name in combination with any one or more of the following data elements, when the data element is not encrypted, redacted or secured by any other method rendering the element unreadable or unusable:

- Social Security Number;
- Number on a driver license issued pursuant to § 28-3166 or number on a nonoperating identification license issued pursuant to § 28-3165; or
- Account number or credit card number or debit card number in combination with any required security code, access code, or password that would permit access to the individual's financial account.

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	PI does not include publicly available information that is lawfully made available to the general public from the federal, state, or local government. **Notice Required.** Notice may be provided by one of the following methods: • Written notice; • Telephonic notice; or • Electronic notice if the Entity's primary method of communication with the individual is by electronic means or is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 (E-SIGN Act). **Substitute Notice Available.** If the Entity can demonstrate that the cost of providing notice will exceed $50,000 or that the affected class of persons to be notified exceeds 100,000, or the Entity does not have sufficient contact information. Substitute notice shall consist of all of the following: • Email notice if the Entity has email addresses for the individuals subject to the notice; • Conspicuous posting of the notice on the Web site of the Entity if the Entity maintains one; and • Notification to major statewide media. **Exception: Compliance with Other Laws.** • **Primary Regulator.** Notification pursuant to laws, rules, regulations, guidance, or guidelines established by an Entity's primary or functional state regulator is sufficient for compliance. • **Gramm-Leach-Bliley Act.** The provisions of this statute shall not apply to any Entity who is subject to the provisions of Title V of the Gramm-Leach-Bliley Act. • **HIPAA-Covered Entities.** A provider of health care, health care service plan, health insurer, or a covered entity governed by the medical privacy and security rules issued by the federal Department of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) shall be deemed in compliance with this chapter. **Other Key Provisions:** • **Delay for Law Enforcement.** Notice may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation. Notice required by the statute must be made after the law enforcement agency determines that notification will no longer impede the investigation. • **AG Enforcement.** The state AG may seek actual damages for willful and knowing violations, as well as a civil penalty not to exceed $10,000 per breach or series of similar breaches.

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

Arkansas

Ark. Code § 4-110-101 *et seq*.

S.B. 1167 (signed into law March 31, 2005, Act 1526)

Effective August 12, 2005

[back to table of contents]

Application. Any person, business or state agency (collectively, Entity) that acquires, owns, or licenses computerized data that includes PI.

- The provisions governing maintenance of PI are applicable to any Entity maintaining information on AR residents, whether or not organized or licensed under the laws of AR.

Security Breach Definition. An unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of PI maintained by an Entity.

- Good-faith acquisition of PI by an employee or agent of the Entity for the legitimate purposes of the Entity is not a breach of the security of the system if the PI is not otherwise used or subject to further unauthorized disclosure.

Notification Obligation. Any Entity to which the statute applies shall disclose any breach of the security of the system following discovery or notification of the breach of the security of the system to any resident of AR whose unencrypted PI was, or is reasonably believed to have been, acquired by an unauthorized person.

- Notification is not required if after a reasonable investigation the Entity determines there is no reasonable likelihood of harm to consumers.

Third-Party Data Notification. If an Entity maintains computerized data that includes PI that the Entity does not own that Entity shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery if the PI was, or is reasonably believed to have been, acquired by an unauthorized person.

Timing of Notification. The disclosure shall be made in the most expedient time and manner possible and without unreasonable delay, subject to any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system.

Personal Information Definition. An individual's first name, or first initial and his or her last name, in combination with any one or more of the following data elements when either the name or the data element is not encrypted or redacted:

- Social Security Number;
- Driver license number or AR identification card number;
- Account number or credit card number or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; or
- Medical information (any individually identifiable information, in electronic or physical form, regarding the individual's medical history or medical treatment or diagnosis by a health care professional).

Notice Required. Notice may be provided by one of the following methods:

- Written notice; or
- Electronic mail notice if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 (E-SIGN Act).

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	Substitute Notice Available. If the Entity demonstrates that the cost of providing notice would exceed $250,000, or that the affected class of persons to be notified exceeds 500,000, or the Entity does not have sufficient contact information. Substitute notice shall consist of all of the following: • Email notice when the Entity has email addresses for the subject persons; • Conspicuous posting of the notice on the Web site of the Entity if the Entity maintains one; and • Notification to statewide media. **Exception: Own Notification Policy.** Any Entity that maintains its own notification procedures as part of an information security policy for the treatment of PI and is otherwise consistent with the timing requirements of the statute shall be deemed to be in compliance with the notification requirements of the statute if the Entity notifies affected persons in accordance with its policies in the event of a security breach. **Other Key Provisions:** • **Delay for Law Enforcement.** Notice may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation. Notice required by the statute must be made after the law enforcement agency determines that notification will no longer impede the investigation. • **AG Enforcement.**

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

California

Cal. Civ. Code § 1798.29; 1798.80 *et seq*.

S.B. 1386 (signed into law September 25, 2002)

Effective July 1, 2003

S.B. 24 (signed into law August 31, 2011)

Effective January 1, 2012

S.B. 46 (signed into law September 27, 2013)

Effective January 1, 2014

AB-1710 (signed into law September 30, 2014)

Effective January 1, 2015

A.B. 964, S.B. 570, S.B. 34 (signed into law October 6, 2015)

Effective January 1, 2016

[back to table of contents]

Application. Any person, business, or state agency (collectively, Entity) that does business in CA and owns or licenses computerized data that contains PI.

- The provisions governing maintenance of PI that the Entity does not own appear applicable to any Entity maintaining information on CA residents, whether or not the Entity conducts business in CA.

Security Breach Definition. An unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of PI maintained by the Entity.

- Good-faith acquisition of PI by an employee or agent of the Entity for the purposes of the Entity is not a breach of the security of the system, provided that the PI is not used or subject to further unauthorized disclosure.

Notification Obligation. Any Entity to which the statute applies shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any CA resident whose unencrypted PI was, or is reasonably believed to have been, acquired by an unauthorized person.

Attorney General Notification. If an Entity is required to notify more than 500 CA residents, the Entity shall electronically submit a single sample copy of the notification, excluding any personally identifiable information, to the Attorney General.

Third-Party Data Notification. If an 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 the security of the data immediately following discovery if the PI was, or is reasonably believed to have been, acquired by an unauthorized person.

Timing of Notification. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

Personal Information Definition.

(1) An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted (meaning rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security):

- Social Security Number;
- Driver license number or CA identification card number;
- Account number or credit card number or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account;
- Medical information (any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional);
- Health insurance information (an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	information in an individual's application and claims history, including any appeals records); or • Information or data collected through the use or operation of an automated license plate recognition system (a searchable computerized database resulting from the operation of one or more mobile or fixed cameras combined with computer algorithms to read and convert images of registration plates and the characters they contain into computer-readable data). (2) User name or email address, in combination with a password or security question and answer that would permit access to an online account. PI does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. **Notice Required.** Notice may be provided by one of the following methods: • Written notice; or • Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 (E-SIGN Act). For breaches of login credentials for an email account furnished by the Entity, notice may not be provided to the breached email address, but may be provided by one of the following methods: • Written notice; • Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 (E-SIGN Act); or • Clear and conspicuous notice delivered to the CA resident online when the CA resident is connected to the online account from an IP address or online location from which the Entity knows the CA resident customarily accesses the account. The notice shall be written in plain language and shall include a description of the following: • The date of the notice; • Name and contact information of the reporting person or Entity; • Type of PI subject to the unauthorized access and acquisition; • The date, estimated date, or date range during which the breach occurred, if it can be determined; • Whether notification was delayed as a result of law enforcement investigation, if that can be determined; • A general description of the breach incident, if that information is possible to determine at the time the notice is provided; • The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number. • If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months, along with all information necessary to take advantage of the offer to

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

any person whose information was or may have been breached if the breach exposed or may have exposed personal information involving social security numbers, driver's license, or CA identification card numbers.

At the Entity's discretion, the notice may also include:

- Information about what the Entity has done to protect individuals whose information has been breached;
- Advice on steps that the person whose information was breached may take to protect him or herself

For breaches of only user name or email address, in combination with a password or security question and answer that would permit access to an online account, notice may be provided in electronic or other form and should direct CA residents to:

- Promptly change their password, security question or answer, or
- Take other appropriate steps to protect the online account with the Entity and all other online accounts with the same user name or email address and password or security question or answer.

The notice shall be titled "Notice of Data Breach," and shall provide the information above under the headings:

- "What Happened,"
- "What Information Was Involved,"
- "What We Are Doing,"
- "What You Can Do," and
- "More Information."

The notice shall be formatted to call attention to the nature and significance of the information it contains, shall clearly and conspicuously display the title and headings, and shall not contain text smaller than 10-point type. (A model security breach notification form is provided in the statute.)

Substitute Notice Available. If the Entity demonstrates that the cost of providing notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000, or the Entity does not have sufficient contact information. Substitute notice shall consist of all of the following:

- Email notice when the Entity has an email address for the subject persons;
- Conspicuous posting for at least 30 days of the notice on the Entity's Web site if the Entity maintains one (meaning providing a link to the notice on the home page or first significant page after entering the Web site that is in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks that call attention to the link); and
- Notification to major statewide media. State agencies using substitute notice must also notify the California Office of Information Security within the Department of Technology.

Exception: Own Notification Policy. An Entity that maintains its own notification procedures as part of an information security policy for the treatment of PI and is otherwise consistent with the timing requirements of the statute shall be deemed in compliance with the notification requirements of the statute if it notifies subject persons in accordance with its policies in the

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	event of a security breach. **Exception: HIPAA-Covered Entities.** A covered entity under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) will be deemed to have complied with the notice requirements in this state law if it has complied with the notice requirements in Section 13402(f) of the Health Information Technology for Economic and Clinical Health Act (HITECH). **Other Key Provisions:** • **Delay for Law Enforcement.** Notification may be delayed if the law enforcement agency determines that the notification will impede a criminal investigation. The notification required by the statute shall be made promptly after the law enforcement agency determines that it will not compromise the investigation. • **Private Right of Action.** Any customer injured by a violation of this title may institute a civil action to recover damages. In addition, any business that violates, proposes to violate, or has violated this title may be enjoined. • **Waiver Not Permitted.**

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

Colorado

Colo. Rev. Stat. § 6-1-716

H.B. 1119 (signed into law April 24, 2006)

Effective September 1, 2006

[back to table of contents]

Application. Any individual or commercial entity (collectively, Entity) that conducts business in CO and that owns or licenses computerized data that includes PI.

- The provisions governing maintenance of PI that the Entity does not own appear applicable to any Entity maintaining information on CO residents, whether or not the Entity conducts business in CO.

Security Breach Definition. An unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of PI maintained by an Entity.

- Good-faith acquisition of PI by an employee or agent of an Entity for the purposes of the Entity is not a breach of the security of the system if the PI is not used for or is not subject to further unauthorized disclosure.

Notification Obligation. An Entity that conducts business in CO and that owns or licenses computerized data that includes PI about a resident of CO shall, when it becomes aware of a breach of the security of the system, give notice as soon as possible to the affected CO resident.

- Notification is not required if after a good-faith, prompt and reasonable investigation, the Entity determines that misuse of PI about a CO resident has not occurred and is not likely to occur.

Notification to Consumer Reporting Agencies. If an Entity is required to notify more than 1,000 CO residents, the Entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the anticipated date of the notification to the residents and the approximate number of residents who are to be notified. This paragraph shall not apply to a person who is subject to Title V of the Gramm-Leach-Bliley Act.

Third-Party Data Notification. If an Entity maintains computerized data that includes PI that the 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 of the security of the system immediately following discovery of a breach, if misuse of 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.

Timing of Notification. Notice shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.

Personal Information Definition. A CO resident's first name or first initial and last name in combination with any one or more of the following data elements that relate to the resident, when the data elements are not encrypted, redacted, or secured by any other method rendering the name or the element unreadable or unusable:

- Social Security Number;
- Driver license number or other identification card number; or
- Account number or credit card number or debit card number in combination with any required security code, access code, or password that would permit access to a financial account.

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	PI does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media. **Notice Required.** Notice may be provided by one of the following methods: • Written notice to the postal address listed in the Entity's records; • Telephonic notice; or • Electronic notice, if a primary means of communication by the Entity with a CO resident is by electronic means or the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 (E-SIGN Act). **Substitute Notice Available.** If the Entity demonstrates that the cost of providing notice will exceed $250,000, or that the affected class of persons to be notified exceeds 250,000 CO residents, or the Entity does not have sufficient contact information to provide notice. Substitute notice shall consist of all of the following: • Email notice if the Entity has email addresses for the members of the affected class of CO residents; • Conspicuous posting of the notice on the Web site of the Entity if the Entity maintains one; and • Notification to major statewide media. **Exception: Own Notification Policy.** Any Entity that maintains its own notification procedures as part of an information security policy for the treatment of PI and whose procedures are otherwise consistent with the timing requirements of the statute shall be deemed to be in compliance with the notice requirements of the statute if the Entity notifies affected CO customers in accordance with its policies in the event of a breach of the security of the system. **Exception: Compliance with Other Laws.** • **Primary Regulator.** Notification pursuant to laws, rules, regulations, guidance, or guidelines established by an Entity's primary or functional state regulator is sufficient for compliance. • **Gramm-Leach-Bliley Act.** The provisions of this statute shall not apply to any Entity who is subject to Title V of the Gramm-Leach-Bliley Act. **Other Key Provisions:** • **Delay for Law Enforcement.** Notice may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation and the law enforcement agency has notified the Entity that conducts business in CO not to send notice required by the statute. • **AG Enforcement.** The AG may seek direct damages and injunctive relief.

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

Connecticut

Conn. Gen. Stat. § 36a-701b

S.B. 650 (signed into law June 8, 2005, Public Act 05-148)

Effective January 1, 2006

H.B. 6001 (signed into law June 15, 2012, Public Act 12-1)

Effective October 1, 2012

S.B. 949 (signed into law June 11, 2015)

Effective Oct. 1, 2015

[back to table of contents]

Application. Any person, business or agency (collectively, Entity) that conducts business in CT, and who, in the ordinary course of such Entity's business, owns, licenses, or maintains computerized data that includes PI.

- The provisions governing maintenance of PI that the Entity does not own appear applicable to any Entity maintaining information on CT residents, whether or not the Entity conducts business in CT.

Security Breach Definition. 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 unusable.

Notification Obligation. Any Entity to which the statute applies shall disclose any breach of security following the discovery of the breach to any CT resident whose PI was breached, or is reasonably believed to have been, breached.

- Notification is not required if, after an appropriate investigation and consultation with relevant federal, state, and local agencies responsible for law enforcement, the Entity reasonably determines that the breach will not likely result in harm to the individuals whose PI has been acquired and accessed.

Notification Obligation to Attorney General. Any Entity that is required under the statute to notify CT residents of any breach of security shall not later than the time when notice is provided to the resident also provide notice of the breach of security to the Attorney General.

Third-Party Data Notification. If an Entity maintains computerized data that includes PI that the Entity does not own the Entity shall notify the owner or licensee of the information of any breach of the security of the data immediately following its discovery if the PI was, or is reasonably believed to have been, breached.

Timing of Notification. The disclosure shall be made without unreasonable delay, **[Effective Oct. 1, 2015:** but not later than ninety days after the discovery of such breach, unless a shorter time is required under federal law], consistent with any measures necessary to determine the nature and scope of the breach, to identify individuals affected, or to restore the reasonable integrity of the data system.

Personal Information Definition. An individual's first name or first initial and last name in combination with any one or more of the following data elements:

- Social Security Number;
- Driver license number or state identification card number; or
- Account number or credit card number or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.

PI does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.

Notice Required. Notice may be provided by one of the following methods:

- Written notice;

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

- Telephonic notice; or
- Electronic notice, provided it is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 (E-SIGN Act).

[Effective Oct. 1, 2015:] A person who conducts business in CT, and who, in the ordinary course of such person's business, owns or licenses computerized data that includes Personal Information, shall offer to each resident whose Personal Information that includes social security numbers was breached or is reasonably believed to have been breached, appropriate identity theft prevention services and, if applicable, identity theft mitigation services. Such service or services shall be provided at no cost to such resident for a period of not less than twelve months. Such person shall provide all information necessary for such resident to enroll in such service or services and shall include information on how such resident can place a credit freeze on such resident's credit file.

Substitute Notice Available. If the Entity demonstrates that the cost of providing notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000 persons, or the Entity does not have sufficient contact information. Substitute notice shall consist of all the following:

- Email notice when the Entity has an email address for the affected persons;
- Conspicuous posting of the notice on the Web site of the Entity if the Entity maintains one; and
- Notification to major statewide media, including newspapers, radio and television.

Exception: Own Notification Policy. Any Entity that maintains its own security breach procedures as part of an information security policy for the treatment of PI and otherwise complies with the timing requirements of the statute shall be deemed to be in compliance with the security breach notification requirements of the statute, provided such Entity notifies subject persons in accordance with its policies in the event of a breach of security.

Exception: Compliance with Other Laws.

- **Primary Regulator.** Notification pursuant to laws, rules, regulations, guidance, or guidelines established by an Entity's primary or functional state regulator is sufficient for compliance.

Other Key Provisions:

- **Delay for Law Enforcement.** Notice may be delayed for a reasonable period of time if a law enforcement agency determines that the notice will impede a criminal investigation and such law enforcement agency has made a request that notification be delayed. Notice required by the statute must be made after the law enforcement agency determines that notification will no longer impede the investigation and so notifies the Entity of such determination.
- **AG Enforcement.** The AG may seek direct damages and

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	injunctive relief. • **Notice to the Insurance Department.** Pursuant to Bulletin IC-25 (Aug. 18, 2010), all licensees and registrants of the Connecticut Insurance Department are required to notify the Department of any information security incident which affects any CT residents as soon as the incident is identified, but no later than five calendar days after the incident is identified.

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

Delaware

Del. Code Ann. tit. 6 § 12B-101 *et seq*.

H.B. 116 (signed into law June 28, 2005)

Effective June 28, 2005

H.B. 247 (signed into law June 10, 2010)

Effective June 10, 2010

[back to table of contents]

Application. Any individual or commercial entity (collectively, Entity) that conducts business in DE and that owns or licenses computerized data that includes PI about a resident of DE.

- The provisions governing maintenance of PI that the Entity does not own appear applicable to any Entity maintaining information on DE residents, whether or not the Entity conducts business in DE.

Security Breach Definition. An unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of PI maintained by an Entity.

- Good-faith acquisition of PI by an employee or agent of an Entity for the purposes of the Entity is not a breach of the security of the system, provided that the PI is not used or subject to further unauthorized disclosure.

Notification Obligation. Any Entity to which the statute applies shall, when it becomes aware of a breach of the security of the system, notify the affected DE resident.

- Notification is not required if after a good-faith, reasonable, and prompt investigation the Entity determines there is no reasonable likelihood of harm to consumers.

Third-Party Data Notification. An Entity that maintains computerized data that includes PI that the Entity does not own or license shall give notice to and cooperate with the owner or licensee of the information of any breach of the security of the system immediately following discovery of the breach, if misuse of PI about a DE resident occurred or is reasonably likely to occur. Cooperation includes sharing with the owner or licensee information relevant to the breach.

Timing of Notification. Notice shall be made in good faith, in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.

Personal Information Definition. A DE resident's first name or first initial and last name, in combination with any one or more of the following data elements that relate to the resident, when either the name or the data elements are not encrypted:

- Social Security Number;
- Driver license number or DE identification card number; or
- Account number or credit card number or debit card number in combination with any required security code, access code, or password that would permit access to a resident's financial account.

PI does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Notice Required. Notice may be provided by one of the following methods:

- Written notice;
- Telephonic notice; or
- Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	15 U.S.C. § 7001 (E-SIGN Act). **Substitute Notice Available.** If the Entity demonstrates that the cost of providing notice will exceed $75,000, or that the affected class of DE residents to be notified exceeds 100,000 residents, or the Entity does not have sufficient contact information to provide notice. Substitute notice shall consist of all of the following: • Email notice if the Entity has email addresses for the members of the affected class of DE residents; • Conspicuous posting of the notice on the Web site of the Entity if the Entity maintains one; and • Notice to major statewide media. **Exception: Own Notification Policy.** An Entity that maintains its own notification procedures as part of an information security policy for the treatment of PI, and whose procedures are otherwise consistent with the timing requirements of the statute, is deemed to be in compliance with the notice requirements of the statute if the Entity notifies affected DE residents in accordance with its policies in the event of a breach of the security of the system. **Exception: Compliance with Other Laws.** • Primary Regulator. Notification pursuant to laws, rules, regulations, guidance, or guidelines established by an Entity's primary or functional state regulator is sufficient for compliance. **Other Key Provisions:** • **Delay for Law Enforcement.** Notice may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation. Notice required by the statute must be made without unreasonable delay and as soon as possible after the law enforcement agency determines that notification will no longer impede the investigation. • **AG Enforcement.** The Attorney General may bring an action to address violations of this chapter and for other relief that may be necessary to ensure compliance and recover direct economic damages.

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

District of Columbia

D.C. Code § 28-3851 *et seq*.

Council Bill 16-810 (signed into law March 8, 2007)

Effective July 1, 2007

[back to table of contents]

Application. Any person or entity (collectively, Entity) who conducts business in DC and who, in the course of such business, owns or licenses computerized or other electronic data that includes PI.

- The provisions governing maintenance of PI that the Entity does not own appear applicable to any Entity maintaining information on DC residents, whether or not the Entity conducts business in DC.

Security Breach Definition. An unauthorized acquisition of computerized or other electronic data, or any equipment or device storing such data that compromises the security, confidentiality, or integrity of PI maintained by the Entity.

- Acquisition of data that has been rendered secure, so as to be unusable by an unauthorized third party, shall not be deemed to be a breach of the security of the system.
- Good-faith acquisition of PI by an employee or agent of the Entity for the purposes of the Entity is not a breach of the security of the system if the PI is not used improperly or subject to further unauthorized disclosure.

Notification Obligation. Any Entity to which the statute applies, and who discovers a breach of the security system, shall promptly notify any DC resident whose PI was included in the breach.

Notification to Consumer Reporting Agencies. If any Entity is required to notify more than 1,000 persons of a breach of security, the Entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by section § 603(p) of the federal Fair Credit Reporting Act, of the timing, distribution and content of the notices. This subsection shall not apply to an Entity who is required to notify consumer reporting agencies of a breach pursuant to Title V of the Gramm-Leach-Bliley Act.

Third-Party Data Notification. Any Entity that maintains, handles, or otherwise possesses computerized or other electronic data that includes PI that the Entity does not own shall notify the owner or licensee of the information of any breach of the security of the system in the most expedient time possible following discovery.

Timing of Notification. The notification shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

Personal Information Definition. Any number or code or combination of numbers or codes, such as account number, security code, access code, or password, that allows access to or use of an individual's financial or credit account, or an individual's first name or first initial and last name, or phone number, or address, and any one or more of the following data elements:

- Social Security Number;
- Driver license number or DC identification card number; or
- Credit card number or debit card number.

"Personal information" shall not include publicly available information that is lawfully made available to the general public from federal, state, or local government records

Notice Required. Notice may be provided by one of the following methods:

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	• Written notice; or • Electronic notice, if the customer has consented to receipt of electronic notice consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 (E-SIGN Act). **Substitute Notice Available.** If the Entity demonstrates that the cost of providing notice to persons would exceed $50,000, that the number of persons to receive notice under the statute exceeds 100,000, or that the Entity does not have sufficient contact information. Substitute notice shall consist of all of the following: • Email notice when the Entity has an email address for the subject persons; • Conspicuous posting of the notice on the Web site of the Entity if the Entity maintains one; and • Notice to major local and, if applicable, national media. **Exception: Own Notification Policy.** Any Entity that maintains its own notification procedures as part of an information security policy for the treatment of PI and whose procedures are otherwise consistent with the timing requirements of the statute shall be deemed in compliance with the notification requirements of the statute if the Entity provides notice, in accordance with its policies, reasonably calculated to give actual notice to persons to whom notice is otherwise required to be given under the statute. • Notice under this section may be given by email if the Entity's primary method of communication with the DC resident is by email. **Exception: Compliance with Other Laws.** • **Gramm-Leach-Bliley Act.** The provisions of this statute shall not apply to any Entity who is subject to the provisions of Title V of the Gramm-Leach-Bliley Act. **Other Key Provisions:** • **Delay for Law Enforcement.** Notice may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation. Notice required by the statute must be made without unreasonable delay and as soon as possible after the law enforcement agency determines that notification will no longer impede the investigation. • **AG Enforcement.** The AG may seek direct damages and injunctive relief. • **Private Right of Action.** Any District of Columbia resident injured by a violation may institute 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. • **Waiver Not Permitted.**

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

Florida

Fla. Stat. § 501.171

S.B. 1524 (signed into law June 20, 2014)

Effective July 1, 2014

S.B. 1526 (signed into law June 20, 2014)

Effective July 1, 2014

[back to table of contents]

Application. A sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity that acquires, maintains, stores, or uses personal information (collectively, Entity).

An entity that has been contracted to maintain, store, or process personal information on behalf of an Entity or governmental entity ("third-party agent").

Security Breach Definition. The unauthorized access of data in electronic form containing personal information.

- Good-faith access of PI by an employee or agent of the Entity is not a breach of the security of the system, provided the information is not used for a purpose unrelated to the business or subject to further unauthorized use.

Notification to Individuals. Entity must give notice to each individual in Florida whose PI was, or the Entity reasonably believes to have been, accessed as a result of the breach.

Notice to affected individuals is not required if, after an appropriate investigation and consultation with relevant federal, state, or local law enforcement agencies, the Entity reasonably determines that the breach has not and will not likely result in identity theft or any other financial harm to the individuals whose PI has been accessed. Such a determination must be documented in writing and maintained for at least 5 years. The Entity must provide the written determination to the Department within 30 days after the determination.

Attorney General Notification. Entity must provide notice to the Department of Legal Affairs (Department) of any breach of security affecting 500 or more individuals in Florida.

Notification to Consumer Reporting Agencies. If an Entity discovers circumstances requiring notification pursuant to this section of more than 1,000 persons at a single time, the Entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution, and content of the notices.

Third-Party Data Notification. Any third-party agent shall disclose to the Entity for which the information is maintained any breach of the security of the system as soon as practicable, but no later than 10 days following the determination of the breach or reason to believe the breach occurred. Upon receiving notice from a third-party agent, the Entity for which the information is maintained shall provide notices to the Department and Affected Individuals. A third-party agent must provide the Entity with all information that the Entity needs to comply with notice requirements. A third-party agent may provide notice to the Department or Affected Individuals on behalf of the Entity; however, a third-party agent's failure to provide proper notice shall be deemed a violation against the Entity.

Timing of Notification.

- To the Department: Notice must be provided as expeditiously as practicable, but no later than 30 days after the determination of the breach or reason to believe a breach occurred.
- To the Individuals: Notice must be made as expeditiously as practicable and without unreasonable delay, taking into account the time necessary to allow the Entity to determine the scope of the breach of security, to identify individuals affected by the breach, and

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

to restore the reasonable integrity of the data system that was breached, but no later than 30 days after the determination of a breach or reasons to believe a breach occurred. Entity may receive 15 additional days to provide notice to Individuals if good cause for delay is provided in writing to the Department within 30 days after determination of the breach or reason to believe a breach occurred.

Personal Information Definition.

- An individual's first name or first initial and last name in combination with any one or more of the following data elements for that individual:
  - Social Security Number;
  - A driver license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity;
  - A financial account number or credit or debit card number in combination with any required security code, access code, or password that is necessary to permit access to an individual's financial account;
  - Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or
  - An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual.
- A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account.

PI does not include publicly available information that is made publicly available by a federal, state, or local governmental entity. The term also does not include information that is encrypted, secured, or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable.

Notice Required. Notice may be provided by one of the following methods:

- To the Department:
  - Written notice must include:
    - A synopsis of the events surrounding the breach at the time notice is provided.
    - The number of individuals in Florida who were or potentially have been affected by the breach.
    - Any services related to the breach being offered or scheduled to be offered, without charge, by the Entity to individuals, and instructions as to how to use such services.
    - A copy of the notice required to affected individuals or an explanation of the other actions taken to give notice to affected individuals.
    - The name, address, telephone number, and e-mail address of the employee or agent of the Entity from whom additional information may be obtained about the breach.

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

- Upon the Department's request, the Entity must provide the following information to the Department:
  - A police report, incident report, or computer forensics report.
  - A copy of the policies in place regarding breaches.
  - Steps that have been taken to rectify the breach.
- The Entity may provide supplemental information regarding a breach at any time to the Department.

- To Affected Individuals:
  - Notice must contain, at a minimum:
    - The date, estimated date, or estimated date range of the breach.
    - A description of the PI that was accessed or reasonably believed to have been accessed as a part of the breach.
    - Information that the individual can use to contact the Entity to inquire about the breach and the personal information that the Entity maintained about the individual.
  - Notice may be provided by the following methods:
    - Written notice sent to the mailing address of the individual in the records of the Entity; or
    - E-mail notice sent to the individual's e-mail address in the Entity's records.

Substitute Notice to Affected Individuals Available. If the Entity demonstrates that the cost of providing notice would exceed $250,000, the affected class of subject persons to be notified exceeds 500,000, or the Entity does not have sufficient contact information. Substitute notice shall consist of both of the following:

- Conspicuous posting of the notice on the Entity's Web site, if the Entity maintains one; and
- Notification in print and to broadcast media, including major media in urban and rural areas where the Affected Individuals reside.

Penalties. An Entity that violates the statute in the following manner is subject to the following administrative fines:

- A violation of this section shall be treated as an unfair or deceptive trade practice in any action brought by the Department against a Entity or third-party agent.
- An Entity that fails to notify the Department or Affected Individuals shall be liable for a civil penalty not to exceed $500,000, (i) in the amount of $1,000 for each day the breach goes undisclosed for up to 30 days and, thereafter, $50,0000 for each 30-day period or portion therefore for up to 180 days; or (ii) if the violation continues for more than 180 days, in an amount not to exceed $500,000. The civil penalties under this paragraph apply per breach, and not per individual affected by the breach.

Exception: Compliance with Other Laws.

- **Primary Regulator.** Notification pursuant to laws, rules, regulations, guidance, or guidelines established by an Entity's primary or functional state regulator is sufficient for compliance.

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	Other Key Provisions: • **Delay for Law Enforcement.** Notice to Individuals may be delayed for a specified period that the law enforcement agency determines is reasonably necessary in a written request if a law enforcement agency determines that the notice will impede a criminal investigation. Law enforcement agency may, by a subsequent written request, revoke such delay as of a specified date or extend the period specified in the original request made to a specified date if further delay is necessary. • **Public Records Exemption.** All information received by the Department pursuant to the notification requirements or pursuant to a law enforcement or Department investigation is confidential and exempt from the Public Records requirement under the State Constitution and statutes.

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

Georgia

Ga. Code § 10-1-910 *et seq.*

S.B. 230 (signed into law May 5, 2005)

Effective May 5, 2005

S.B. No. 236 (signed into law May 24, 2007)

Effective May 24, 2007

[back to table of contents]

Application. 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 PI to nonaffiliated third parties, or any state or local agency or subdivision thereof including any department, bureau, authority, public university or college, academy, commission, or other government entity (collectively, Entity) that maintains computerized data that includes PI of individuals. The statute shall not apply to any governmental agency whose records are maintained primarily for traffic safety, law enforcement, or licensing purposes or for purposes of providing public access to court records or to real or personal property information.

- The provisions governing maintenance of PI are applicable to any Entity maintaining information on GA residents, whether or not organized or licensed under the laws of GA.

Security Breach Definition. An unauthorized acquisition of an individual's electronic data that compromises the security, confidentiality, or integrity of PI of such individual maintained by an Entity.

- Good-faith acquisition or use of PI by an employee or agent of an Entity for the purposes of such Entity is not a breach of the security of the system, provided that the PI is not used or subject to further unauthorized disclosure.

Notification Obligation. Any Entity that maintains computerized data that includes PI of individuals shall give notice of any breach of the security of the system following discovery or notification of the breach to any resident of GA whose unencrypted PI was, or is reasonably believed to have been, acquired by an unauthorized person.

Notification to Consumer Reporting Agencies. In the event an Entity discovers circumstances requiring notification of more than 10,000 residents of GA at one time, the Entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution, and content of the notices.

Third-Party Data Notification. If an Entity maintains computerized data on behalf of another Entity that includes PI of individuals that the Entity does not own, it shall notify the other Entity of any breach of the security of the system within 24 hours following discovery, if the PI was, or is reasonably believed to have been, acquired by an unauthorized person.

Timing of Notification. The notice shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.

Personal Information Definition. An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:

- Social Security Number;
- Driver license or state identification card number;
- Account number or credit card number or debit card number if circumstances exist wherein such a number could be used without additional identifying information, access codes, or passwords;

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	• Account passwords or personal identification numbers or other access codes; or • Any of the above items when not in connection with the individual's first name or first initial and last name, if the information compromised would be sufficient to perform or attempt to perform identity theft against the person whose information was compromised. PI does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. **Notice Required.** Notice may be provided by one of the following methods: • Written notice; or • Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 (E-SIGN Act). **Substitute Notice Available.** If an Entity demonstrates that the cost of providing notice would exceed $50,000, that the affected class of individuals to be notified exceeds 100,000, or that the Entity does not have sufficient contact information to provide written or electronic notice to such individuals. Substitute notice shall consist of all of the following: • Email notice, if the Entity has an email address for the individuals to be notified; • Conspicuous posting of the notice on the Entity's Web site, if the Entity maintains one; and • Notification to major statewide media. **Exception: Own Notification Policy.** Any Entity that maintains its own notification procedures as part of an information security policy for the treatment of PI and whose procedures are otherwise consistent with the timing requirements of the statute shall be deemed to be in compliance with the notification requirements of the statute if it notifies the individuals who are the subjects of the notice in accordance with its policies in the event of a breach of the security of the system. **Other Key Provisions:** • **Delay for Law Enforcement.** Notice may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation. Notice required by the statute must be made without unreasonable delay and as soon as possible after the law enforcement agency determines that notification will no longer impede the investigation.

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

Hawaii

H.R.S. § 487N-1 *et seq*.

S.B. 2290 (signed into law May 25, 2006, Act 135)

Effective January 1, 2007

S.B. 2402 (signed into law April 17, 2008, Act 19)

Effective April 17, 2008

[back to table of contents]

Application. Any sole proprietorship, partnership, corporation, association, or other group, however organized, and whether or not organized to operate at a profit, including financial institutions organized, chartered, or holding a license or authorization certificate under the laws of HI, any other state, the United States, or any other country, or the parent or the subsidiary of any such financial institution, and any entity whose business is records destruction, or any government agency that collects PI for specific government purposes (collectively, Entity) that owns or licenses PI of residents of HI in any form (whether computerized, paper, or otherwise).

- The provisions governing maintenance of PI are applicable to any Entity maintaining information on HI residents, whether or not the Entity conducts business in HI.

Security Breach Definition. Any unauthorized access to and acquisition of unencrypted or unredacted records or data containing PI where illegal use of the PI has occurred, or is reasonably likely to occur, where such unauthorized access and acquisition creates a risk of harm to a person. 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.

- Good-faith acquisition of PI by an employee or agent of the Entity for a legitimate purpose is not a security breach, provided that the PI is not used for a purpose other than a lawful purpose of the business and is not subject to further unauthorized disclosure.

Notification Obligation. Any Entity to which the statute applies shall provide notice to the affected person of a security breach following discovery or notification of the breach.

Attorney General/Agency Notification. If more than 1,000 persons are notified at one time under this section, the business shall notify the State of Hawaii's Office of Consumer Protection of the timing, content, and distribution of the notice.

Notification to Consumer Reporting Agencies. If more than 1,000 persons are notified at one time pursuant to this section, the Entity shall notify in writing, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution, and content of the notice.

Notification Obligation for Government Agencies. A government agency shall submit a written report to the legislature within 20 days after discovery of a security breach at the government agency that details information relating to the nature of the breach, the number of individuals affected by the breach, a copy of the notice of security breach that was issued, the number of individuals to whom the notice was sent, whether the notice was delayed due to law enforcement considerations, and any procedures that have been implemented to prevent the breach from reoccurring. In the event that a law enforcement agency informs the government agency that notification may impede a criminal investigation or jeopardize national security, the report to the legislature may be delayed until 20 days after the law enforcement agency has determined that notice will no longer impede the investigation or jeopardize national security.

Third-Party Data Notification. Any business located in HI or any business that conducts business in HI that maintains or possesses records or data containing PI of residents of HI that the business does not own or license,

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	shall notify the owner or licensee of the PI of any security breach immediately following discovery of the breach. **Timing of Notification.** The disclosure notification shall be made without unreasonable delay, consistent with any measures necessary to determine sufficient contact information, determine the scope of the breach, and restore the reasonable integrity, security, and confidentiality of the data system. **Personal Information Definition.** An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: • Social Security Number; • Driver license number or HI identification card number; or • Account number, credit card number, debit card number, access code, or password that would permit access to an individual's financial account. PI does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. **Notice Required.** Notice may be provided by one of the following methods: • Written notice to the last available address the Entity has on record; • Telephonic notice, provided that contact is made directly with the affected persons; or • Email notice, for those persons for whom an Entity has a valid email address and who have agreed to receive communications electronically if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 (E-SIGN Act). The notice shall be clear and conspicuous and shall include a description of the following: • The incident in general terms; • Type of PI subject to the unauthorized access and acquisition; • The general acts of the Entity to protect the PI from further unauthorized access; • A telephone number that the person may call for further information and assistance, if one exists; and • Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports. **Substitute Notice Available.** If the Entity demonstrates that the cost of providing notice would exceed $100,000, or that the affected class of persons to be notified exceeds 200,000, or if the Entity does not have sufficient contact information or consent to satisfy the required notice, for only those affected persons without sufficient contact information or consent, or if the Entity is unable to identify particular affected persons, for only those unidentifiable affected persons. Substitute notice shall consist of <u>all</u> the following: • Email notice when the Entity has an email address for the subject persons; • Conspicuous posting of the notice on the Entity's Web site, if the

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	Entity maintains one; and • Notification to major statewide media. **Exception: Compliance with Other Laws.** • **Federal Interagency Guidance.** A financial institution that is subject to and in compliance with the Federal Interagency Guidance Response Programs for Unauthorized Access to Customer Information and Customer Notice, issued on March 7, 2005, by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision, and any revisions, additions, or substitutions relating to said interagency guidance, shall be deemed to be in compliance. • **HIPAA-Covered Entities.** A provider of health care, health care service plan, health insurer, or a covered entity governed by the medical privacy and security rules issued by the federal Department of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) shall be deemed in compliance with this chapter. **Penalties.** Any Entity that violates any provisions of the statute is subject to penalties of not more than $2,500 for each violation. **Other Key Provisions:** • **Delay for Law Enforcement.** Notice may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation or jeopardize national security and requests a delay; provided that such request is made in writing, or the Entity documents the request contemporaneously in writing, including the name of the law enforcement officer making the request and the officer's law enforcement agency engaged in the investigation. The notice shall be provided without unreasonable delay after the law enforcement agency communicates to the Entity its determination that notice will no longer impede the investigation or jeopardize national security. • **AG Enforcement.** • **Waiver Not Permitted.**

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

Idaho

Idaho Code § 28-51-104 *et seq*.

S.B. 1374 (signed into law March 30, 2006, Chapter 258)

Effective July 1, 2006

H.B. 566 (signed into law March 31, 2010)

Effective July 1, 2010

[back to table of contents]

Application. Any agency, individual or commercial entity (collectively, Entity) that conducts business in ID and that owns or licenses computerized data that includes PI about a resident of ID.

- The provisions governing maintenance of PI that the Entity does not own appear applicable to any Entity maintaining information on ID residents, whether or not the Entity conducts business in ID.

Security Breach Definition. An illegal acquisition of unencrypted computerized data that materially compromises the security, confidentiality, or integrity of PI for one or more persons maintained by Entity.

- Good-faith acquisition of PI by an employee or agent of an Entity for the purposes of the Entity is not a breach of the security of the system, provided that the PI is not used or subject to further unauthorized disclosure.

Notification Obligation. An Entity to which the statute applies shall give notice as soon as possible to the affected ID resident.

- Notification is 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.

Notification Obligation for State Agencies. When an agency becomes aware of a security breach, it shall, within 24 hours, notify the office of the ID Attorney General.

- A state agency must also report a security breach to the office of the chief information officer within the department of administration, pursuant to the information technology resource management council policies.

Third-Party Data Notification. An Entity that maintains computerized data that includes PI that the Entity does not own or license shall give notice to and cooperate with the owner or licensee of the information of any breach of the security of the system immediately following discovery of the breach, if misuse of PI about an ID resident occurred or is reasonably likely to occur. Cooperation includes sharing with the owner or licensee information relevant to the breach.

Timing of Notification. Notice must be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach, to identify the individuals affected, and to restore the reasonable integrity of the computerized data system.

Personal Information Definition. An ID resident's first name or first initial and last name in combination with any one or more of the following data elements that relate to the resident, when either the name or the data elements are not encrypted:

- Social Security Number;
- Driver license number or Idaho identification card number; or
- Account number or credit card number in combination with any required security code, access code, or password that would permit access to a resident's financial account.

"Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

Notice Required. Notice may be provided by one of the following methods:

- Written notice to the most recent address the Entity has in its records;
- Telephonic notice; or
- Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 (E-SIGN Act).

Substitute Notice Available. If the Entity required to provide notice demonstrates that the cost of providing notice would exceed $25,000, or that the number of ID residents to be notified exceeds 50,000, or that the Entity does not have sufficient contact information to provide notice. Substitute notice consists of all of the following:

- Email notice if the Entity has email addresses for the affected ID residents;
- Conspicuous posting of the notice on the Web site of the Entity if the Entity maintains one; and
- Notice to major statewide media.

Exception: Own Notification Policy. Any Entity that maintains its own notice procedures as part of an information security policy for the treatment of PI, and whose procedures are otherwise consistent with the timing requirements of the statute is deemed to be in compliance with the notice requirements if the Entity notifies affected ID residents in accordance with its policies in the event of a breach of the security of the system.

Exception: Compliance with Other Laws.

- **Primary Regulator.** Notification pursuant to laws, rules, regulations, guidance, or guidelines established by an Entity's primary or functional state regulator is sufficient for compliance.

Penalties. Any Entity that intentionally fails to give notice in accordance with the statute shall be subject to a fine of not more than $25,000 per breach of the security of the system.

Penalties for Government Disclosure. Any governmental employee that intentionally discloses personal information not subject to disclosure otherwise allowed by law shall be subject to a fine of not more than $2,000, by imprisonment in the county jail for a period of not more than 1 year, or both.

Other Key Provisions:

- **Delay for Law Enforcement.** Notice may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation. Notice required by the statute must be made as soon as possible after the law enforcement agency determines that notification will no longer impede the investigation.
- **Primary State Regulator Enforcement.** Authorizes primary state regulator to bring a civil action against an Entity that it believes to have violated the statute by failing to give notice to enforce compliance with the statute and enjoin the Entity from

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	further violation.

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

Illinois

815 Ill. Comp. Stat. 530/5, 530/10, 530/12, 530/15, 530/20, 530/25

H.B. 1633 (signed into law June 16, 2005, Public Act 94-36)

Effective June 27, 2006

H.B. 3025 (signed Aug. 22, 2011, Public Act 97-483)

Effective Jan. 1, 2012

H.B. 1260 (signed into law May 6, 2016)

Effective January 1, 2017

[back to table of contents]

Application. Any data collector, which 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 PI (collectively, Entity) that owns or licenses PI concerning an IL resident.

- The provisions governing maintenance of PI that the Entity does not own appear applicable to any Entity maintaining information on IL residents, whether or not the Entity conducts business in IL.

Security Breach Definition. An unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of PI maintained by the Entity.

- Good-faith acquisition of PI by an employee or agent of the Entity for a legitimate purpose of the Entity does not constitute a security breach, provided that the PI is not used for a purpose unrelated to the Entity's business or subject to further unauthorized disclosure.

Notification Obligation. Any Entity to which the statute applies shall notify the resident at no charge that there has been a breach following discovery or notification of the breach. **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.

Notification Obligation for State Agencies. Any state agency that collects PI and has had a breach of security of the system data or written material shall submit a report within five business days of the discovery or notification of the breach to the General Assembly listing the breaches and outlining any corrective measures that have been taken to prevent future breaches. Any agency that has submitted a report under the statute shall submit an annual report listing all breaches of security and the corrective measures that have been taken to prevent future breaches.

[Effective Jan. 1, 2017: State agencies must report security breaches involving more than 250 Illinois residents to the Attorney General, including the types of personal information compromised. the number of Illinois residents affected. any steps the agency has taken or plans to take to notify consumers. the date and timeframe of the breach, if known. Such notification must be made within 45 days of the agency's discovery of the security breach or when the agency provides notice to consumers, whichever is sooner, unless there is good cause for reasonable delay to determine the scope of the breach and restore the integrity, security, and confidentiality of the data system, or when law enforcement requests in writing to withhold disclosure of some or all of the information required in the notification. If the date or timeframe of the breach is unknown at the time the notice is sent to the Attorney General, the State agency shall send the Attorney General the date or timeframe of the breach as soon as possible.**]**

Third-Party Data Notification. Any Entity that maintains or stores computerized data that includes PI that the Entity does not own or license shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the PI was, or is reasonably believed to have been, acquired by an unauthorized person. In addition, such Entities shall cooperate with the data owner or licensee in matters relating to the breach, including (1) giving notice of the (approximate) date and nature of the breach and (2) informing the owner or licensee of

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	steps taken or planned relating to the breach. **Timing of Notification.** The disclosure notification shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system. **Personal Information Definition.** Either of the following: (1) An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted or **[effective Jan. 1, 2017:** are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the name or data elements have been acquired without authorization through the breach of security**]**: • Social Security Number; • Driver license number or State identification card number; or • Account number or credit card number or debit card number or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account. • **[Effective Jan. 1, 2017:** • Medical information (any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional, including such information provided to a website or mobile application) • Health insurance information (health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any medical information in an individual's health insurance application and claims history, including any appeals records) • Unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee to authenticate an individual, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data.**]** **[Effective Jan. 1, 2017**: (2) user name or email address, in combination with a password or security question and answer that would permit access to an online account, when either the user name or email address or password or security question and answer are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the data elements have been obtained through the breach of security.**]** PI does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. **Notice Required.** Notice may be provided by one of the following methods: • Written notice; • Electronic notice, if consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 (E-SIGN Act); or • **[Effective Jan. 1, 2017:** For breaches involving user name/email and password/security questions only, in "electronic or other

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	form."] **Contents of Notice.** For breach of personal information other than user name/email and password/security question, the notice shall include: • The toll-free numbers and addresses for consumer reporting agencies; • The toll-free number, address, and website address for the Federal Trade Commission; and • A statement that the individual can obtain information from these sources about fraud alerts and security freezes. The notice shall not include the number of Illinois residents affected by the breach. **[Effective Jan. 1, 2017:** For breach of personal information involving user name/email and password/security questions, notice may be provided in electronic or other form directing the Illinois resident whose personal information has been breached to promptly change his or her user name or password and security question or answer, as applicable, or to take other steps appropriate to protect all online accounts for which the resident uses the same user name or email address and password or security question and answer.**]** **Substitute Notice Available.** If the Entity demonstrates that the cost of providing notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000, or the Entity does not have sufficient contact information. Substitute notice shall consist of <u>all</u> of the following: • Email notice if the Entity has an email address for subject persons; • Conspicuous posting of the notice on the Entity's Web site if the Entity maintains one; and • Notification to major statewide media. or, **[effective Jan. 1, 2017:** if the breach impacts residents in one geographic area, to prominent local media in areas where affected individuals are likely to reside if such notice is reasonably calculated to give actual notice to persons whom notice is required.**]** **Exception: Own Notification Policy.** An Entity that maintains its own notification procedures as part of an information security policy for the treatment of PI and is otherwise consistent with the timing requirements of the statute, shall be deemed in compliance with the notification requirements of the statute if the Entity notifies subject persons in accordance with its policies in the event of a breach of the security of the system data. **Exception: Compliance with Other Laws**. **[Effective Jan. 1, 2017**: Any Entity that is subject to and in compliance with the privacy and security standards under the Health Insurance Portability and Accountability Act of 1996 and the Health Information Technology for Economic and Clinical Health Act (HITECH) shall be deemed to be in compliance, provided that any Entity required to provide notification of a breach to the Secretary of Health and Human Services pursuant to HITECH also provides such notification to the Attorney General within 5 business days of notifying the Secretary.**]**

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	Other Key Provisions: • **Delay for Law Enforcement.** Notice may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation and provides the Entity with a written request of delay. Notice required by the statute must be made without unreasonable delay and as soon as possible after the law enforcement agency determines that notification will no longer impede the investigation. • **Waiver Not Permitted.** • Violation of the statute constitutes an unlawful practice under the IL Consumer Fraud and Deceptive Business Practices Act.

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

Indiana

Ind. Code § 4-1-11 *et seq.*; § 24-4.9-1 *et seq*.

S.B. 503 (signed into law April 26, 2005, Act 503)

Effective July 1, 2006

H.E.A. No. 1197 (signed into law March 24, 2008)

H.E.A. No. 1121 (signed into law May 12, 2009)

Effective July 1, 2009

[back to table of contents]

Application. Any individual, corporation, business trust, estate, trust, partnership, association, nonprofit corporation or organization, cooperative, state agency or any other legal entity (collectively, Entity) that owns or licenses computerized data that includes PI.

- The provisions governing maintenance of PI are applicable to any Entity maintaining information on IN residents, whether or not organized or licensed under the laws of IN.

Security Breach Definition. An unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of PI maintained by an Entity. The term includes the unauthorized acquisition of computerized data that has been transferred to another medium, including paper, microfilm, or a similar medium, even if the transferred data are no longer in a computerized format.

- Unauthorized acquisition of a portable electronic device on which PI is stored does not constitute a security breach if all PI on the device is protected by encryption and the encryption key: (i) has not been compromised or disclosed, and (ii) is not in the possession of or known to the person who, without authorization, acquired or has access to the portable electronic device.
- Good-faith acquisition of PI by an employee or agent of the Entity for lawful purposes of the Entity does not constitute a security breach if the PI is not used or subject to further unauthorized disclosure.

Notification Obligation. Any Entity, after discovering or being notified of a breach of the security of data, shall disclose the breach to an IN resident whose unencrypted PI was or may have been acquired by an unauthorized person or whose encrypted PI was or may have been acquired by an unauthorized person with access to the encryption key if the Entity knows, or should know, or should have known that the unauthorized acquisition constituting the breach has resulted in or could result in identity deception (as defined in IND. CODE § 35-43-5-3.5), identity theft, or fraud affecting the IN resident.

Attorney General Notification. If the Entity makes such a disclosure, the data base owner shall also disclose the breach to the attorney general.

Notification to Consumer Reporting Agencies. An Entity required to make a disclosure to more than 1,000 consumers shall also disclose to all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis information necessary to assist the consumer reporting agency in preventing fraud, including PI of an IN resident affected by the breach of the security of a system.

Third-Party Data Notification. An Entity that maintains computerized data that includes PI but that does not own or license the PI shall notify the owner of the PI if the Entity discovers that PI was or may have been acquired by an unauthorized person.

Timing of Notification. The disclosure notification shall be made without unreasonable delay and consistent with any measures necessary to determine the scope of the breach and restore the integrity of the system.

Personal Information Definition. A Social Security Number that is not encrypted or redacted, or an individual's first and last names, or first initial and last name, and one or more of the following data elements that are not encrypted or redacted:

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	• A driver license number or state identification card number; • A credit card number; or • A financial account number or debit card number in combination with a security code, password, or access code that would permit access to the person's account. PI does 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. **Notice Required.** Notice may be provided by one of the following methods: • Mail; • Telephone; • Fax; or • Email, if the Entity has the email address of the affected IN resident. State agencies are subject to slightly different notice requirements. **Substitute Notice Available.** If an Entity demonstrates that the cost of the disclosure exceeds $250,000, or that the affected class of subject persons to be notified exceeds 500,000. Substitute notice shall consist of all of the following: • Conspicuous posting of the notice on the Web site of the Entity, if the Entity maintains one; and • Notice to major news reporting media in the geographic area where IN residents affected by the breach of the security of a system reside. **Exception: Own Notification Policy.** Any Entity that maintains its own disclosure procedures as part of an information privacy policy or a security policy is not required to make a separate disclosure under the statute if the Entity's information privacy policy or security policy is at least as stringent as the disclosure requirements under the statute. **Exception: Compliance with Other Laws.** This section does not apply to an Entity that maintains its own data security procedures as part of an information privacy, security policy, or compliance plan under: • The Gramm-Leach-Bliley Act; • The Health Insurance Portability and Accountability Act of 1996 (HIPAA); • The USA Patriot Act (P.L. 107-56); • Executive Order 13224; • The Driver Privacy Protection Act (18 U.S.C. § 2781 *et seq*.); or • The Fair Credit Reporting Act (15 U.S.C. § 1681 *et seq*.) if the Entity's information privacy, security policy, or compliance plan requires the Entity to maintain reasonable procedures to protect and safeguard from unlawful use or disclosure PI of IN residents that is collected or maintained by the Entity and the Entity complies with the Entity's information privacy, security policy, or compliance plan. **Other Key Provisions:**

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	• **AG Enforcement.** A person that knowingly or intentionally fails to comply with the database maintenance obligations commits a deceptive act that is actionable only by the state AG. Penalties include injunctive relief, a civil penalty of not more than $150,000 per violation, and reasonable costs.

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

Iowa

Iowa Code § 715C.1-2

2007 S.F. 2308 (signed into law May 9, 2008)

Effective July 1, 2008

2014 S.F. 2259 (signed into law April 3, 2014)

Effective July 1, 2014

[back to table of contents]

Application. Any individual, corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture, government, governmental subdivision, agency, or instrumentality, public corporation, or any other legal or commercial entity (collectively, Entity) that owns or licenses computerized data that includes an IA resident's PI that is used in the course of the Entity's business, vocation, occupation, or volunteer activities and that was subject to a breach of security.

Security Breach Definition. Unauthorized acquisition of PI maintained in computerized form by an Entity that compromises the security, confidentiality, or integrity of the PI. Also, unauthorized acquisition of PI maintained by a person in any medium, including on paper, that was transferred by the person to that medium from computerized form and that compromises the security, confidentiality, or integrity of the PI.

- Good-faith acquisition of PI by an Entity or that Entity's employee or agent for a legitimate purpose of that Entity is not a breach of security, provided that the PI is not used in violation of applicable law or in a manner that harms or poses an actual threat to the security, confidentiality, or integrity of the PI.

Notification Obligation. Any Entity to which the statute applies shall give notice of the breach of security following discovery of such breach of security, or receipt of notification of such breach, to any IA resident whose PI was included in the information that was breached.

- Notification is not required if, after an appropriate investigation or after consultation with the relevant federal, state, or local agencies responsible for law enforcement, the Entity determines that no reasonable likelihood of financial harm to the IA residents whose PI 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.

Attorney General Notification. If an Entity owns or licenses computerized data that includes a consumer's personal information that is used in the course of the Entity's business, vocation, occupation, or volunteer activities suffers a security breach requiring notification of more than 500 Iowa residents than the Entity will give written notice following discovery of such breach, or receipt of notification required by third parties, to the director of the consumer protection division of the Attorney General's Office. Notice or receipt of notice must be provided within 5 business days of giving notice to any consumer.

Third-Party Data Notification. Any Entity who maintains or otherwise possesses PI on behalf of another Entity shall notify the owner or licensor of the information of any breach of security immediately following discovery of such breach if an IA resident's PI was included in the information that was breached.

Timing of Notification. The notification shall be made in the most expeditious manner possible and without unreasonable delay, consistent with any measures necessary to sufficiently determine contact information for the affected IA residents, determine the scope of the breach, and restore the reasonable integrity, security, and confidentiality of the data.

Personal Information Definition. An individual's first name or first initial and last name in combination with any one or more of the following data elements that relate to the individual if any of the data elements are not encrypted,

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	redacted, or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable or are encrypted, redacted, or otherwise altered by any method or technology but the keys to unencrypt, unredact, or otherwise read the data elements have also been obtained through the breach of security: • Social Security Number; • Driver license number or other unique identification number created or collected by a government body; • Account number or credit card number or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; • Account number or credit card number or debit card number in combination with any *required expiration date*, security code, access code, or password that would permit access to an individual's financial account; • Unique electronic identifier or routing code, in combination with any required security code, access code, or password that would permit access to an individual's financial account; or • Unique biometric data, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data. PI does not include information that is lawfully obtained from publicly available sources, or from federal, state, or local government records lawfully made available to the general public. . **Notice Required.** Notice shall include, at a minimum, <u>all</u> of the following: • A description of the breach of security; • The approximate date of the breach of security; • The type of PI obtained as a result of the breach of security; • Contact information for consumer reporting agencies; and • Advice to the consumer to report suspected incidents of identity theft to local law enforcement or the attorney general. Notification may be provided by one of the following methods: • Written notice to the last available address the Entity has in the Entity's records; or • Electronic notice if the Entity's customary method of communication with the resident is by electronic means or is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 (E-SIGN Act). **Substitute Notice Available.** If the Entity demonstrates that the cost of providing notice would exceed $250,000, that the affected class of IA residents to be notified exceeds 350,000 persons, or if the Entity does not have sufficient contact information to provide notice. Substitute notice shall consist of the following: • Electronic mail notice when the Entity has an electronic mail address for the affected IA residents; • Conspicuous posting of the notice or a link to the notice on the

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	Entity's Web site, if the Entity maintains one; and • Notification to major statewide media. **Exception: Own Notification Policy.** Any Entity that maintains its own disclosure procedures as part of an information privacy policy or a security policy is not required to make a separate disclosure under the statute if the Entity's information privacy policy or security policy is at least as stringent as the disclosure requirements under the statute. **Exception: Compliance with Other Laws.** • **Federal Regulator.** This statute does not apply to an Entity that complies with notification requirements or breach of security procedures that provide greater protection to PI and at least as thorough disclosure requirements than that provided by this section pursuant to the rules, regulations, procedures, guidance, or guidelines established by the Entity's primary or functional federal regulator. • **More Protective Law.** This statute does not apply to an Entity that complies with a state or federal law that provides greater protection to PI and at least as thorough disclosure requirements for breach of security or PI than that provided by the statute. • **Gramm-Leach-Bliley Act.** This statute does not apply to an Entity that is subject to and complies with regulations promulgated pursuant to Title V of the Gramm-Leach-Bliley Act. **Other Key Provisions:** • **Delay for Law Enforcement.** The consumer notification requirements of this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation and the agency has made a written request that the notification be delayed. The notification required by this section shall be made after the law enforcement agency determines that the notification will not compromise the investigation and notifies the Entity required to give notice in writing. • **AG Enforcement.**

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

Kansas

Kan. Stat. § 50-7a01 *et seq*.

S.B. 196 (signed into law April 19, 2006)

Effective January 1, 2007

[back to table of contents]

Application. Any individual, partnership, corporation, trust, estate, cooperative, association, government, or governmental subdivision or agency or other entity (collectively, Entity) that conducts business in KS and that owns or licenses computerized data that includes PI.

- The provisions governing maintenance of PI that the Entity does not own appear applicable to any Entity maintaining information on KS residents, whether or not the Entity conducts business in KS.

Security Breach Definition. Any unauthorized access to and acquisition of unencrypted or unredacted computerized data that compromises the security, confidentiality, or integrity of PI maintained by an Entity and that causes, or such Entity reasonably believes has caused or will cause, identity theft to any consumer.

- Good-faith acquisition of PI by an employee or agent of an Entity for the purposes of the Entity is not a breach of the security of the system, provided that the PI is not used for or is not subject to further unauthorized disclosure.

Notification Obligation. Any Entity to which the statute applies shall, when it becomes aware of any breach of the security of the system, give notice as soon as possible to the affected KS resident.

- Notification is 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.

Notification to Consumer Reporting Agencies. In the event that an Entity must notify more than 1,000 consumers at one time, the Entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution and content of the notices.

Third-Party Data Notification. An Entity that maintains computerized data that includes PI that the Entity does not own or license shall give notice to the owner or licensee of the information of any breach of the security of the data following discovery of a breach, if the PI was, or is reasonably believed to have been, accessed and acquired by an unauthorized person.

Timing of Notification. Notice must be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.

Personal Information Definition. A consumer's first name or first initial and last name linked to any one or more of the following data elements that relate to the consumer, when the data elements are neither encrypted nor redacted:

- Social Security Number;
- Driver license number or state identification card number; or
- Account number or credit card number or 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.

PI does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Notice Required. Notice may be provided by one of the following methods:

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	• Written notice; or • Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 (E-SIGN Act). **Substitute Notice Available.** If the Entity required to provide notice demonstrates that the cost of providing notice will exceed $100,000, or that the affected class of consumers to be notified exceeds 5,000, or that the Entity does not have sufficient contact information to provide notice. Substitute notice shall consist of all of the following: • Email notice, if the Entity has email addresses for the affected class of consumers; • Conspicuous posting of the notice on the Entity's Web site if the Entity maintains one; and • Notification to major statewide media. **Exception: Own Notification Policy.** An Entity that maintains its own notification procedures as part of an information security policy for the treatment of PI, and whose procedures are otherwise consistent with the timing requirements of the statute, is deemed to be in compliance with the notice requirements of the statute if the Entity notifies affected consumers in accordance with its policies in the event of a breach of security of the system. **Exception: Compliance with Other Laws.** • **Primary Regulator.** Notification pursuant to laws, rules, regulations, guidance, or guidelines established by an Entity's primary or functional state or federal regulator is sufficient. **Other Key Provisions:** • **Delay for Law Enforcement.** Notice may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation. Notice shall be made in good faith, without unreasonable delay and as soon as possible after the law enforcement agency determines that notification will no longer impede the investigation. • **AG Enforcement.** Allows the state AG (or insurance commissioner in the case of an insurance company) to bring actions at law or equity to enforce compliance and enjoin future violations.

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

Kentucky

KY Rev. Stat. §365.732

H.B. 232 (signed into law April 10, 2014)

Effective July 15, 2014

H.B. 5 (signed into law April 10, 2014)

Effective January 1, 2015

[back to table of contents]

Application. "Information holder" defined as any person or business entity that conducts business in the state (collectively, Entity). Specific notification obligations also apply to "non-affiliated third parties" (NTP) of state and municipal government agencies and public educational institutions that receive or collect and maintain personal information from the agencies and institutions pursuant to a contract.

Security Breach Definition. The unauthorized acquisition of unencrypted, unredacted computerized data that compromises the security, confidentiality, or integrity of PI maintained by the Entity as part of a database regarding multiple individuals that actually causes, or leads the Entity to believe has caused or will cause, identity theft or fraud against any Kentucky resident.

- Good faith acquisition of PI by an employee or agent of the Entity for the purposes of the Entity is not a breach of the security of the system if the PI is not used or subject to further unauthorized disclosures.

Notification Obligation.

- Any Entity to which the statute applies must, upon discovery or notification of breach in the security system, notify any Kentucky resident whose unencrypted information was or is reasonably believed to have been acquired by an unauthorized person.
- In the case of an NTP's security system breach, the contracting agency or institution must notify the Attorney General within 72 hours of being notified by the NTP. Private entities do not have an obligation to notify any state regulatory authority.

Notification to Consumer Reporting Agencies. If an Entity discovers circumstances requiring notification pursuant to this section of more than 1,000 persons at one time, the Entity shall also notify, without unreasonable delay, all consumer reporting agencies and credit bureaus that compile and maintain files on consumers on nationwide basis, as defined by 15 U.S.C. § 1681a, of the timing, distribution, and content of the notices.

Third-Party Data Notification.

- An Entity that maintains computerized data that includes PI that the Entity does not own shall notify the owner or licensee of the information of any breach of the security of the data as soon as reasonably practicable following discovery, if the PI was or is reasonably believed to have been acquired by an unauthorized person.
- An NTP, upon discovery or notification of breach in the security system, must notify its contracting agency or institution in the most expedient time possible and without unreasonable delay, within 72 hours of determining that a breach occurred. (NTPs following federal law or regulation regarding breach investigation and notice may satisfy this obligation by providing a copy of any federally required reports or investigations to the contracting agency or institution.) The contracting agency or institution bears the responsibility of notifying

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

any affected individuals.

Timing of Notification.

- Notice should occur in the most expedient time possible and without unreasonable delay, subject to 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.
- NTP's notice should occur in the most expedient time possible and without unreasonable delay, within 72 hours of determining that a breach occurred.

Personal Information Definition. An individual's first name or first initial and last name in combination with one or more of the following data elements when the name or data element is not redacted:

- Social Security Number;
- Driver license number; or
- Account number, credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.

For NTPs, “personal information” means an individual's first name or first initial and last name; personal mark; or unique biometric or genetic print or image, in combination with one or more of the following data elements:

- An account number, credit card number, or debit card number, that, in combination with any required security code, access code, or password, would permit access to an account;
- A Social Security number;
- A taxpayer identification number that incorporates a Social Security number;
- A driver's license number, state identification card number, or other individual identification number issued by any agency;
- A passport number of other identification number issued by the United States government; or
- Individually identifiable health information as defined in 45 C.F.R. § 160.103 except for education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. § 1232g.

Obligations under these statutes apply only to unencrypted, unredacted computerized data.

Notice Required. Notice may be provided by one of the following methods:

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

13997061.38

- Written notice;
- Electronic notice, if the notice is provided consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 (E-SIGN Act).

Substitute Notice Available. If the Entity can demonstrate that the cost of providing notice would exceed $250,000, that the number of individuals to be notified exceeds 500,000, or that they do not have sufficient contact information for those affected. Substitute notice shall consist of all of the following:

- E-mail notification if the Entity has e-mail addresses for the affected individuals;
- Conspicuous posting regarding the incident on the Entity's website, if the Entity maintains a website; and
- Notification to major statewide media.

Exception: Own Notification Policy. An Entity that maintains its own notification procedures as part of an information security policy for the treatment of PI, and is otherwise consistent with the timing requirements of this section, shall be deemed to be in compliance with the notification requirements of this section, if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.

Exception: Compliance with Other Laws.

- **Gramm-Leach-Bliley Act; Federal Health Insurance Portability and Accountability Act; Kentucky agency, local governments or political subdivisions.** The provisions of this statute and the requirements for nonaffiliated third parties in KRS Chapter 61 shall not apply to any Entity subject to the provisions of Title V of the Gramm-Leach-Bliley Act, the federal Health Insurance Portability and Accountability Act, any Kentucky agency, or any Kentucky local governments or political subdivisions.

Other Key Provisions:

- **Delay for Law Enforcement**.
  - Entity's notice may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made promptly after the law enforcement agency determines that it will not compromise the investigation.
  - NTP's notice to its contracting agency may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be given to the contracting agency as soon as reasonably feasible.

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	Kentucky Board of Education Regulation. The Kentucky Board of Education may promulgate administrative regulations in accordance with KRS Chapter 13A as necessary to carry out the requirements of this section.

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

Louisiana

La. Rev. Stat. § 51:3071 *et seq*.

La. Admin. Code tit. 16, pt. III, § 701

S.B. 205 (signed into law July 12, 2005, Act 499)

Effective January 1, 2006

[back to table of contents]

Application. Any individual, corporation, partnership, sole proprietorship, joint stock company, joint venture, or any other legal entity that conducts business in LA or that owns or licenses computerized data that includes PI, or any agency that owns or licenses computerized data that includes PI (collectively, Entity).

- The provisions governing maintenance of PI that the Entity does not own appear applicable to any Entity maintaining information on LA residents, whether or not the Entity conducts business in LA.

Security Breach Definition. The compromise of the security, confidentiality, or integrity of computerized data that results in, or there is a reasonable basis to conclude has resulted in, the unauthorized acquisition of and access to PI maintained by an Entity.

- Good-faith acquisition of PI by an employee of the Entity for the purposes of the Entity is not a breach of the security of the system, provided that the PI is not used for, or is not subject to, unauthorized disclosure.

Notification Obligation. Any Entity to which the statute applies shall, following discovery of a breach of the security of the system containing such data, notify any resident of the state whose PI was, or is reasonably believed to have been, acquired by an unauthorized person.

- Notification is not required if after a reasonable investigation the Entity determines that there is not a reasonable likelihood of harm to customers.

Attorney General Notification. When notice to LA citizens is required by the statute, the Entity shall provide written notice detailing the breach of the security of the system to the Consumer Protection Section of the Attorney General's Office. Notice shall include the names of all LA citizens affected by the breach. Notice to the state AG shall be timely if received within 10 days of distribution of notice to LA citizens. Each day notice is not received by the state AG shall be deemed a separate violation.

Third-Party Data Notification. Any individual, corporation, partnership, sole proprietorship, joint stock company, joint venture, or any other legal entity that maintains computerized data that includes PI that the agency or person does not own shall notify the owner or licensee of the information if the PI was, or is reasonably believed to have been, acquired by an unauthorized person through a breach of security of the system containing such data, following discovery by the agency or person of a breach of the security system.

Timing of Notification. The notification required pursuant to the statute shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach, prevent further disclosures, and restore the reasonable integrity of the data system.

Personal Information Definition. An individual's first name or first initial and last name in combination with any one or more of the following data elements, when the name or the data element is not encrypted or redacted:

- Social Security Number;
- Driver license number; or
- Account number or credit card number or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

account.

"Personal information" shall not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Notice Required. Notice may be provided by one of the following methods:

- Written notification; or
- Electronic notification, if the notification provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 (E-SIGN Act).

Substitute Notice Available. If an Entity demonstrates that the cost of providing notification would exceed $250,000, or that the affected class of persons to be notified exceeds 500,000, or the Entity does not have sufficient contact information. Substitute notice shall consist of all of the following:

- Email notification when the Entity has an email address for the subject persons;
- Conspicuous posting of the notification on the Entity's Web site if the Entity maintains one; and
- Notification to major statewide media.

Exception: Own Notification Policy. Any Entity that maintains notification procedures as part of its information security policy for the treatment of PI which is otherwise consistent with the timing requirements of the statute shall be deemed to be in compliance with the notification requirements of the statute if the Entity notifies subject persons in accordance with the policy and procedures in the event of a breach of a security of the system.

Exception: Compliance with Other Laws.

- Federal Interagency Guidance. A financial institution that is subject to and in compliance with the Federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice, issued on March 7, 2005, by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision, and any revisions, additions, or substitutions relating to said interagency guidance, shall be deemed to be in compliance.

Penalties.

- A civil action may be instituted to recover actual damages resulting from the failure to disclose in a timely manner to a person that there has been a breach of the security system resulting in the disclosure of a person's PI.
- Failure to provide timely notice may be punishable by a fine not to exceed $5,000 per violation. Notice to the state AG shall be timely if received within 10 days of distribution of notice to LA citizens. Each day notice is not received by the state AG shall be deemed a separate violation.

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	Other Key Provisions: • **Delay for Law Enforcement.** Notice may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation. Notice required by the statute must be made without unreasonable delay and as soon as possible after the law enforcement agency determines that notification will no longer impede the investigation. • **Private Right of Action.** A civil action may be instituted to recover actual damages resulting from the failure to disclose in a timely manner to a person that there has been a breach of the security system resulting in the disclosure of a person's PI.

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

Maine

10 Me. Rev. Stat. § 1346 *et seq*.

L.D. 1671 (signed into law June 10, 2005, Chapter 379)

Effective January 31, 2006

H.P. 672 (signed into law May 19, 2009, Chapter 161)

Effective May 19, 2009

[back to table of contents]

Application. Any individual, partnership, corporation, limited liability company, trust, estate, cooperative, association or other entity, including agencies of state government, the University of Maine System, the Maine Community College System, Maine Maritime Academy and private colleges and universities, or any information broker, which means 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 PI to nonaffiliated third parties (collectively, Entity) that maintains computerized data that includes PI. The provisions governing maintenance of PI are applicable to any Entity maintaining information on ME residents, whether or not organized or licensed under the laws of ME.

Security Breach Definition. An unauthorized acquisition, release or use of an individual's computerized data that includes PI that compromises the security, confidentiality or integrity of PI of the individual maintained by an Entity.

- Good-faith acquisition, release or use of PI by an employee or agent of an Entity on behalf of the Entity is not a breach of the security of the system if the PI is not used for or subject to further unauthorized disclosure to another person.

Notification Obligation. If an Entity that maintains computerized data that includes PI becomes aware of a breach of the security of the system, the Entity shall give notice of the breach following discovery or notification of the security breach to a resident of ME whose PI has been, or is reasonably believed to have been, acquired by an unauthorized person.

- Notification is not required if after conducting a good-faith, reasonable and prompt investigation, the Entity determines that there is not a reasonable likelihood that the PI has been or will be misused.

Attorney General/State Agency Notification. When notice of a breach of the security of the system is required, the Entity shall notify the appropriate state regulators within the Department of Professional and Financial Regulation, or if the Entity is not regulated by the department, the state AG.

Notification to Consumer Reporting Agencies. If an Entity must notify more than 1,000 persons at a single time, the Entity shall also notify, without unreasonable delay, consumer reporting agencies that compile and maintain files on consumers on a nationwide basis. Notification must include the date of the breach, an estimate of the number of persons affected by the breach, if known, and the actual or anticipated date that persons were or will be notified of the breach.

Third-Party Data Notification. A third party that maintains, on behalf of another Entity, computerized data that includes PI that the third party does not own shall notify the owner of the PI of a breach of the security of the system immediately following discovery if the PI was, or is reasonably believed to have been, acquired by an unauthorized person.

Timing of Notification. The notices must be made as expediently as possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or with measures necessary to determine the scope of the security breach and restore the reasonable integrity, security, and confidentiality of the data in the system. Notification may be delayed for no longer than 7 business days after a law enforcement agency determines

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	that the notification will not compromise a criminal investigation. **Personal Information Definition.** An individual's first name, or first initial, and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted: • Social Security Number; • Driver license number or state identification card number; • Account number or credit card number or debit card number if circumstances exist wherein such a number could be used without additional identifying information, access codes or passwords; • Account passwords or PI numbers or other access codes; or • Any of the above data elements when not in connection with the individual's first name, or first initial, and last name, if the information compromised would be sufficient to permit a person to fraudulently assume or attempt to assume the identity of the person whose information was compromised. "Personal information" does not include information from 3rd-party claims databases maintained by property and casualty insurers or publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media. **Notice Required.** Notice may be provided by one of the following methods: • Written notice; or • Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 (E-SIGN Act). **Substitute Notice Available.** If the Entity maintaining PI demonstrates that the cost of providing notice would exceed $5,000, that the affected class of individuals to be notified exceeds 1,000, or that the person maintaining PI does not have sufficient contact information to provide written or electronic notice to those individuals. Substitute notice shall consist of all of the following: • Email notice, if the Entity has email addresses for the individuals to be notified; • Conspicuous posting of the notice on the Entity's Web site if the Entity maintains one; and • Notification to major statewide media. **Penalties.** Provides for civil penalties in the amount of $500 per violation, up to a maximum of $2,500 per day; equitable relief; or enjoinment from future violations. **Other Key Provisions:** • **Delay for Law Enforcement.** If, after the completion of the required investigation, notification is required under this section, the notification required by this section may be delayed for no longer than seven business days after a law enforcement agency determines that the notification will not compromise a criminal investigation.

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	• **AG Enforcement.** Enforced by state AG and/or where applicable, the Department of Professional and Financial Regulation Office of Consumer Credit Regulation.

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

Maryland

Md. Code Com. Law § 14-3501 *et seq*.

H.B. 208 (signed into law April 3, 2007)

Effective January 1, 2008

[back to table of contents]

Application. A sole proprietorship, partnership, corporation, association, or any other business entity, whether or not organized to operate at a profit, including a financial institution organized, chartered, licensed, or otherwise authorized under the laws of MD, any other state, the United States, or any other country (collectively, Entity) that owns or licenses computerized data that includes PI of an individual residing in MD.

- The provisions governing maintenance of PI are applicable to any Entity maintaining information on MD residents, whether or not organized or licensed under the laws of MD.

Security Breach Definition. The unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of the PI maintained by an Entity.

- A good-faith acquisition of PI by an employee or agent of an Entity for the purposes of the business, provided that the PI is not used or subject to further unauthorized disclosure, does not constitute a security breach.

Notification Obligations. An Entity to which the statute applies, when it discovers or is notified of a breach of the security of the system, shall notify the individual of the breach.

- Notification is not required if after a good-faith, reasonable and prompt investigation the Entity determines that the PI of the individual was not and will not be misused as a result of the breach. If after the investigation is concluded, the Entity determines that notification is not required, the Entity shall maintain records that reflect its determination for three years after the determination is made.

Attorney General Notification. Prior to giving the notification required under the statute, an Entity shall provide notice of a breach of the security of a system to the state Office of the Attorney General.

Notification to Consumer Reporting Agencies. If an Entity must notify 1,000 or more individuals, the Entity also shall notify, without unreasonable delay, each consumer reporting agency that compiles and maintains files on consumers on a nationwide basis of the timing, distribution, and content of the notices.

Third-Party Data Notification. An Entity that maintains computerized data that includes PI that the Entity does not own or license shall notify the owner or licensee of the PI of a breach of the security of the system if it is likely that the breach has resulted or will result in the misuse of PI of an individual residing in MD.

- Notification required by a third-party Entity shall be given as soon as reasonably practicable after the Entity discovers or is notified of the breach of the security of a system.
- A third-party Entity shall share with the owner or licensee information relative to the breach.

Timing of Notification. The notification required shall be given as soon as reasonably practicable, consistent with measures necessary to determine the scope of the breach of the security of a system, identify the individuals affected, or restore the integrity of the system.

Personal Information Definition. An individual's first name or first initial and last name in combination with any one or more of the following data elements, when the name or the data elements are not encrypted, redacted,

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	or otherwise protected by another method that renders the information unreadable or unusable: • Social Security Number; • Driver license number; • Account number or credit card number or debit card number, that in combination with any required security code, access code, or password, would permit access to an individual's financial account; or • An Individual Taxpayer Identification Number. PI does not include (i) publicly available information that is lawfully made available to the general public from federal, state, or local government records; (ii) information that an individual has consented to have publicly disseminated or listed; or (iii) information that is disseminated or listed in accordance with the federal Health Insurance Portability and Accountability Act (HIPAA). **Notice Required.** Notice may be provided by one of the following methods: • Written notice sent to the most recent address of the individual in the records of the business; • Telephonic notice, to the most recent telephone number of the individual in the records of the business; or • Electronic mail to the most recent email address of the individual in the records of the business if the individual has expressly consented to receive email notice. Notification shall include: • To the extent possible, a description of the categories of information that were, or are reasonably believed to have been, acquired by an unauthorized person, including which of the elements of PI were, or are reasonably believed to have been acquired; • Contact information for the business making the notification, including the business's address, telephone number, and toll-free telephone number if one is maintained; • The toll-free telephone numbers and addresses for the major consumer reporting agencies; and • The toll-free telephone numbers, addresses, and Web site addresses for (i) the Federal Trade Commission; and (ii) the state AG, along with a statement that the individual can obtain information from these sources about steps the individual can take to avoid identity theft. **Substitute Notice Available.** If the Entity demonstrates that the cost of providing notice would exceed $100,000, or that the affected class of individuals to be notified exceeds 175,000, or the Entity does not have sufficient contact information to give notice. Substitute notice shall consist of all of the following: • Email notice to an individual entitled to notification, if the business has an email address for the individual to be notified; • Conspicuous posting of the notice on the Entity's Web site if the Entity maintains a Web site; and • Notification to statewide media.

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	Exception: Compliance with Other Laws. • **Primary Regulator.** An Entity that complies with the requirements for notification procedures under the rules, regulations, procedures, or guidelines established by the primary or functional federal or state regulator of the Entity shall be deemed to be in compliance with the statute. • **Gramm-Leach-Bliley Act.** An Entity or the affiliate of an Entity that is subject to and in compliance with the Gramm-Leach-Bliley Act, the federal Interagency Guidelines Establishing Information Security Standards, and the federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, and any revisions, additions, or substitutions, shall be deemed to be in compliance with this subtitle. **Other Key Provisions:** • **Delay for Law Enforcement.** Notice may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation or jeopardize homeland or national security. Notification shall be given as soon as reasonably practicable after the law enforcement agency determines that it will not impede a criminal investigation and will not jeopardize homeland or national security. • **AG Enforcement.** • **Private Right of Action.** Consumers may bring actions under Title 13 of the Maryland Code, the Unfair and Deceptive Trade Practices Act. • **Waiver Not Permitted.**

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

Massachusetts

Mass. Gen. Laws 93H § 1 *et seq*.

201 C.M.R. 17.00

H.B. 4144 (signed into law August 3, 2007)

Effective October 31, 2007

[back to table of contents]

Application. A natural person, corporation, association, partnership or other legal entity, or any agency, executive office, department, board, commission, bureau, division or authority of MA, or any of its branches, or any political subdivision thereof (collectively, Entity) that owns, licenses, maintains or stores data that includes PI about a resident of MA.

- The provisions governing maintenance of PI are applicable to any Entity maintaining information on MA residents, whether or not organized or licensed under the laws of MA.

Security Breach Definition. 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, maintained by an Entity that creates a substantial risk of identity theft or fraud against a MA resident.

- A good-faith but unauthorized acquisition of PI by an Entity, or employee or agent thereof, for the lawful purpose of such Entity, is not a breach of security unless the PI is used in an unauthorized manner or subject to further unauthorized disclosure.

Notification Obligation. An Entity to which the statute applies shall provide notice to the affected residents, as soon as practicable and without unreasonable delay, when the Entity knows or has reason to know of a breach of security, or when the Entity knows or has reason to know that the PI of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose. Note: MA 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.

Attorney General/State Agency Notification. Notice must be provided to the state Attorney General and the director of consumer affairs and business regulation.

- Upon receipt of notice, the director of consumer affairs and business regulation shall identify any relevant consumer reporting agency or state agency and forward the names of the identified consumer reporting agencies and state agencies to the notifying Entity. The Entity shall, as soon as practicable and without unreasonable delay, also provide notice to consumer reporting agencies and state agencies identified by the director of consumer affairs and business regulation.

Notification Obligation of an Agency Within the Executive Department. If an agency is within the executive department, it shall provide written notification of the nature and circumstances of the breach or unauthorized acquisition or use of the information to the technology division and the division of public records as soon as practicable and without unreasonable delay following discovery of the breach of security or unauthorized acquisition or use, and shall comply with all policies and procedures adopted by that division pertaining to the reporting and investigation of such an incident.

Third-Party Data Notification. An Entity that maintains or stores, but does not own or license data that includes PI about a resident of MA, shall provide notice, as soon as practicable and without unreasonable delay, when such Entity (i) knows or has reason to know of a breach of security or (ii) when the Entity knows or has reason to know that the PI of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose, to

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	the owner or licensor. Such Entity shall cooperate with the owner or licensor of such PI. Cooperation shall include, but not be limited to: (i) informing the owner or licensor of the breach of security or unauthorized acquisition or use, (ii) the date or approximate date of such incident and the nature thereof, and (iii) any steps the Entity has taken or plans to take relating to the incident, except that such cooperation shall not be deemed to require the disclosure of confidential business information or trade secrets, or to provide notice to a resident that may not have been affected by the breach of security or unauthorized acquisition or use. **Timing of Notification.** The notification shall be given as soon as practicable and without unreasonable delay following discovery of the breach. **Personal Information Definition.** A 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 relates to such resident: • Social Security Number; • Driver license or state-issued identification card number; or • Financial account number, or credit card number, with or without any required security code, access code, personal ID number or password, that would permit access to a resident's financial account. PI does 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. **Notice Required.** Notice may be provided by one of the following methods: • Written notice; or • Electronic notice, if notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 (E-SIGN Act). The notice to be provided to the AG, director of consumer affairs, and consumer reporting agencies or state agencies, if any, shall include, but not be limited to: (i) the nature of the breach of security or unauthorized acquisition or use, (ii) the number of residents of MA affected by such incident at the time of notification, and (iii) any steps the Entity has taken or plans to take relating to the incident. Notice to be provided to the resident shall include, but not be limited to: (i) the consumer's rights to obtain a police report, (ii) how to request a security freeze and the necessary information to be provided when requesting the security freeze, and (iii) any fees required to be paid to any of the consumer reporting agencies. The notification shall not include the nature of the breach or unauthorized acquisition or use of the number of residents of MA affected by said breach or unauthorized access or use. **Substitute Notice Available.** If the Entity required to provide notice demonstrates that the cost of providing written notice will exceed $250,000, or that the affected class of MA residents to be notified exceeds 500,000 residents, or the Entity does not have sufficient contact information to provide notice. Substitute notice shall consist of all of the following: • Email notice, if the Entity has email addresses for the members of the affected class of MA residents; • Clear and conspicuous posting of the notice on the home page of

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	the Entity's Web site if the Entity maintains one; and • Publication in or broadcast through media or medium that provides notice throughout MA. **Exception: Compliance with Other Laws.** • **Primary Regulator.** Notification pursuant to laws, rules, regulations, guidance, or guidelines established by an Entity's primary or functional state or federal regulator is sufficient for compliance. **Other Key Provisions:** • **Delay for Law Enforcement.** Notice may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation and has notified the AG, in writing, thereof and informs the Entity of such determination. Notice required by the statute must be made without unreasonable delay and as soon as possible after the law enforcement agency determines that notification will no longer impede the investigation. The Entity shall cooperate with law enforcement in its investigation of any breach of security or unauthorized acquisition or use, which shall include the sharing of information relevant to the incident; provided, however, that such disclosure shall not require the disclosure of confidential business information or trade secrets. • **AG Enforcement.** Penalties include civil penalties, damages, and injunctive relief.

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

Michigan

Mich. Comp. Laws § 445.63, 72 *et seq*.

S.B. 309 (signed into law December 30, 2006, Pub. Act. 566)

Effective July 2, 2007

S.B. No. 223 (signed into law December 21, 2010)

Effective April 1, 2011.

[back to table of contents]

Application. Any individual, partnership, corporation, limited liability company, association, or other legal entity, or any department, board, commission, office, agency, authority, or other unit of state government of MI (collectively, Entity) that owns or licenses data including PI of a MI resident.

- The provisions governing maintenance of PI are applicable to any Entity maintaining information on MI residents, whether or not organized or licensed under the laws of MI.

Security Breach Definition. The unauthorized access and acquisition of data that compromises the security or confidentiality of PI maintained by an 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 Entity, is not a breach of security unless the PI is misused or disclosed to an unauthorized person. In making this determination an Entity shall act with the care an ordinarily prudent Entity in a like position would exercise under similar circumstances.

Notification Obligation. An Entity to which the statute applies shall provide notice of the breach to each resident of MI if (i) the resident's unencrypted and unredacted PI was accessed and acquired by an unauthorized person or (ii) the resident's PI was accessed and acquired in encrypted form by a person with unauthorized access to the encryption key.

- Notification is not required if the Entity determines that the security 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 MI.

This section does not apply to the access or acquisition by a person or agency of federal, state, or local government records or documents lawfully made available to the general public.

Notification to Consumer Reporting Agencies. If an Entity notifies 1,000 or more Michigan residents, the Entity shall, after notifying those residents, notify each consumer reporting agency that compiles and maintains files on consumers on a nationwide basis of the security breach without unreasonable delay. A notification under this subsection shall include the number and timing of notices that the person or agency provided to residents of this state. This subsection does not apply if the person or agency is subject to Title V of the Gramm-Leach-Bliley Act.

Third-Party Data Notification. An Entity that maintains a database that includes data that the Entity does not own or license that discovers a breach of the security of the database shall provide a notice to the owner or licensor of the information of the security breach, unless the Entity determines that the security 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 MI.

Timing of Notification. The notification shall be given without unreasonable delay following discovery of the breach, consistent with measures necessary to determine the scope of the breach of the security of a system or restore the integrity of the system.

Personal Information Definition. The first name or first initial and last name linked to one or more of the following data elements of a resident of MI:

- Social Security Number;
- Driver license number or state personal identification card

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	number; or • Demand deposit or other financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to any of the resident's financial accounts. **Notice Required.** Notice may be provided by one of the following methods: • Written notice sent to the recipient at the recipient's postal address in the records of the Entity; • Telephonic notice given by an individual who represents the Entity if (i) the notice is not given in whole or in part by use of a recorded message, (ii) the recipient has expressly consented to receive notice by telephone, or if the recipient has not expressly consented to receive notice by telephone, the Entity also provides notice pursuant to the above methods if the notice by telephone does not result in a live conversation between the individual representing the Entity and the recipient within three business days after the initial attempt to provide telephonic notice; or • Written notice sent electronically to the recipient if (i) the recipient has expressly consented to receive electronic notice, (ii) the Entity has an existing business relationship with the recipient that includes periodic email communications and based on those communications the Entity reasonably believes that it has the recipient's current email address, or (iii) the Entity conducts its business primarily through Internet account transactions or on the Internet. A notice under the statute shall: • Be written in a clear and conspicuous manner, and shall clearly communicate the content required; • Describe the security breach in general terms; • Describe the type of PI that is the subject of the unauthorized access or use; • If applicable, generally describe what the agency or person providing the notice has done to protect data from further security breaches; • Include a telephone number where a notice recipient may obtain assistance or additional information; and • Remind notice recipients of the need to remain vigilant for incidents of fraud and identity theft. **Substitute Notice Available.** If the Entity demonstrates that the cost of providing notice would exceed $250,000 or that the Entity has to provide notice to more than 500,000 residents of MI. Substitute notice shall consist of all of the following: • Email notice if the Entity has email addresses for any of the residents of MI who are entitled to receive notice; • Conspicuous posting on the Entity's Web site if the Entity maintains one; and • Notification to major statewide media, which notice shall include a telephone number or Web site address that a person may use

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

to obtain additional assistance and information.

A public utility that sends monthly billing or account statements to its customers may provide notice of a security breach to its customers as provided under the statute or by providing all of the following:

- As applicable, email notice in accordance with the statute;
- Notice to the media reasonably calculated to inform the utility's customers of the breach;
- Conspicuous posting of notice of the security breach on the Web site of the utility; and
- Written notice sent in conjunction with the billing or account statement sent to the customer at his or her postal address in the utility's records.

Exception: Compliance with Other Laws.

- **Federal Interagency Guidance.** A financial institution that is subject to and in compliance with the Federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice, issued on March 7, 2005, by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision, and any revisions, additions, or substitutions relating to said interagency guidance, shall be deemed to be in compliance.
- **HIPAA-Covered Entities.** A provider of health care, health care service plan, health insurer, or a covered entity governed by the medical privacy and security rules issued by the federal Department of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) shall be deemed in compliance with this chapter.

Penalties. Provides for criminal penalties for notice of a security breach that has not occurred, where such notice is given with the intent to defraud. The offense is a misdemeanor, punishable by imprisonment for not more than 30 days or a fine of not more than $250 per violation (or both). (The penalty is the same for second and third violations, except that the fine increases to $500 per violation and $750 per violation, respectively.) Similarly, Entities who distribute an advertisement or make any other solicitation that misrepresents to the recipient that a security breach has occurred that may affect the recipient are punishable by imprisonment for not more than 93 days or a fine of not more than $1,000 per violation (or both). (The penalty is the same for second and third violations, except that the fine increases to $2,000 per violation and $3,000 per violation, respectively.)

Entities who fail to provide notice may be ordered to pay a civil fine of not more than $250 for each failure to provide notice, capped at $750,000 per security breach. These penalties do not affect the availability of civil remedies under state or federal law.

Other Key Provisions:

- **Delay for Law Enforcement.** Notice may be delayed if a law enforcement agency determines that the notice will impede a

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	criminal investigation or jeopardize homeland or national security. Notification shall be given as soon as reasonably practicable after the law enforcement agency determines that it will not impede a criminal investigation and will not jeopardize homeland or national security. • **AG Enforcement.** • Provides that Entities may deliver notice pursuant to an agreement with another Entity, if the agreement does not conflict with the Michigan law.

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

Minnesota

Minn. Stat. § 325E.61

H.F. 2121 (signed into law June 2, 2005, Chapter 167)

Effective January 1, 2006

[back to table of contents]

Application. Any person or business that conducts business in MN, and that owns or licenses data that includes PI.

- The provisions governing maintenance of PI that the Entity does not own appear applicable to any Entity maintaining information on MN residents, whether or not the Entity conducts business in MN.

Security Breach Definition. An unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of PI maintained by the Entity.

- Good-faith acquisition of PI by an employee or agent of the Entity for the purposes of the Entity is not a breach of the security of the system, provided that the PI is not used or subject to further unauthorized disclosure.

Notification Obligation. Any Entity to which the statute applies shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of MN whose unencrypted PI was, or is reasonably believed to have been, acquired by an unauthorized person.

Notification to Consumer Reporting Agencies. If an Entity notifies more than 500 persons at one time, the Entity shall also notify, within 48 hours, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution, and content of the notices.

Third-Party Data Notification. Any Entity that maintains data that includes PI that the Entity does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the PI was, or is reasonably believed to have been, acquired by an unauthorized person.

Timing of Notification. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach, identify the individuals affected, and restore the reasonable integrity of the data system.

Personal Information Definition. An individual's first name or first initial and last name in combination with any one or more of the following data elements, when the data element is not secured by encryption or another method of technology that makes electronic data unreadable or unusable, or was secured and the encryption key, password, or other means necessary for reading or using the data was also acquired:

- Social Security Number;
- Driver license number or MN identification card number; or
- Account number or credit card number or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

PI does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Notice Required. Notice may be provided by one of the following methods:

- Written notice to the most recent available address the Entity has in its records; or
- Electronic notice, if the Entity's primary method of communication

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	with the individual is by electronic means, or if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 (E-SIGN Act). **Substitute Notice Available.** If the Entity demonstrates that the cost of providing notice would exceed $250,000 or that the Entity has to provide notice to more than 500,000 residents, or the Entity does not have sufficient contact information. Substitute notice shall consist of all of the following: • Email notice if Entity has Email address for subject persons; • Conspicuous posting of the notice on the Entity's Website if the Entity maintains one; and • Notification to major statewide media. **Exception: Own Notification Policy.** An Entity that maintains its own notification procedures as part of an information security policy for the treatment of PI and whose procedures are otherwise consistent with the timing requirements of the statute, shall be deemed to be in compliance with the notification requirements of the statute, if the Entity notifies subject persons in accordance with its policies in the event of a breach of security of the system. **Exception: Compliance with Other Laws.** • **HIPAA-Covered Entities.** A provider of health care, health care service plan, health insurer, or a covered entity governed by the medical privacy and security rules issued by the federal Department of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) shall be deemed in compliance with this chapter. **Other Key Provisions:** • **Delay for Law Enforcement.** Notice may be delayed to a date certain if a law enforcement agency determines that the notice will impede a criminal investigation. • **AG Enforcement.** • **Private Right of Action.** • **Waiver Not Permitted.** • Does not apply to any "financial institution," as defined by 15 U.S.C. § 6809(3).

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

Mississippi

Miss. Code § 75-24-29

H.B. 582 (signed into law April 7, 2010)

Effective July 1, 2011

[back to table of contents]

Application. Any person who conducts business in MS and who, in the ordinary course of the person's business functions, owns, licenses, or maintains the PI of any MS resident.

Security Breach Definition. An unauthorized acquisition of electronic files, media, databases or computerized data containing personal information of any MS resident 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.

Notification Obligation. A person who conducts business in MS shall disclose any breach of security to all affected individuals. Notification is not required if, after an appropriate investigation, the person reasonably determines that the breach will not likely result in harm to the affected individuals.

Third-Party Data Notification. A person who maintains computerized data which includes PI that the person does not own or license shall notify the owner or licensee of the information of any breach of security as soon as practical following its discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person for fraudulent purposes.

Timing of Notification. Notice shall be provided without unreasonable delay subject to the completion of an investigation by the person to determine the nature and scope of the incident, to identify the affected individuals, or to restore the reasonable integrity of the system.

Personal Information Definition. An individual's first name or first initial and last name in combination with any one or more of the following data elements, when the data element is not secured by encryption or another method of technology that makes electronic data unreadable or unusable:

- Social Security Number;
- Driver license number or state identification card number; or
- Account number or credit card number or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.

PI does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Notice Required. Notice may be provided by one of the following methods:

- Written notice,
- Telephonic notice, or
- Electronic notice, if the Entity's primary method of communication with the individual is by electronic means, or if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 (E-SIGN Act).

Substitute Notice Available. If the Entity demonstrates that the cost of providing notice would exceed $5,000, that the Entity has to provide notice to more than 5,000 residents, or that the Entity does not have sufficient contact information. Substitute notice shall consist of all of the following:

- Email notice if the Entity has Email addresses for subject

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	persons; • Conspicuous posting of the notice on the Entity's Web site if the Entity maintains one; and • Notification to major statewide media. **Exception: Own Notification Policy.** An Entity that maintains its own notification procedures as part of an information security policy for the treatment of PI and whose procedures are otherwise consistent with the timing requirements of the statute, shall be deemed to be in compliance with the notification requirements of the statute, if the Entity notifies subject persons in accordance with its policies in the event of a breach of security of the system. **Exception: Compliance with Federal Regulations.** • Any person that maintains a security breach procedure pursuant to the rules, regulations, or guidelines established by the primary federal functional regulator shall be deemed to be in compliance with this section, provided the person notifies affected individuals in accordance with the policies or the rules, regulations, procedures, or guidelines. **Other Key Provisions:** • **Delay for Law Enforcement.** Any notification shall be delayed for a reasonable period of time if a law enforcement agency determines that the notification will impede a criminal investigation or national security and the law enforcement agency has made a request that the notification be delayed. Any such delayed notification shall be made after the law enforcement agency determines that notification will not compromise the criminal investigation or national security and so notifies the person of that determination. • **AG Enforcement.** Failure to comply with the requirements of the act shall constitute an unfair trade practice and shall be enforced by the Attorney General.

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

Missouri

Mo. Rev. Stat. § 407.1500

H.B. 62

Effective August 28, 2009

[back to table of contents]

Application. Any individual, corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture, government, governmental subdivision, governmental agency, governmental instrumentality, public corporation, or any other legal or commercial entity (collectively, Entity) that owns or licenses PI of residents of MO or any person that conducts business in MO that owns or licenses PI of a resident of MO.

Security Breach Definition. Unauthorized access to and unauthorized acquisition of PI maintained in computerized form by an Entity that compromises the security, confidentiality, or integrity of the PI.

- Good-faith acquisition of PI by an Entity or that Entity's employee or agent for a legitimate purpose of that Entity is not a breach of security, provided that the PI is not used in violation of applicable law or in a manner that harms or poses an actual threat to the security, confidentiality, or integrity of the PI.

Notification Obligation. Any Entity to which the statute applies shall provide notice to the affected consumer that there has been a breach of security following discovery or notification of the breach.

- Notification is not required if, after an appropriate investigation by the Entity or after consultation with the relevant federal, state, or local agencies responsible for law enforcement, the Entity determines that a risk of identity theft or other fraud to any consumer is not reasonably likely to occur as a result of the breach. Such a determination shall be documented in writing and the documentation shall be maintained for five years.

Notification of Consumer Reporting Agencies. In the event an Entity notifies more than 1,000 consumers at one time pursuant to this section, the Entity shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution, and content of the notice.

Attorney General Notification. In the event an Entity provides notice to more than 1,000 consumers at one time pursuant to this section, the Entity shall notify, without unreasonable delay, the state AG's office of the timing, distribution, and content of the notice.

Third-Party Data Notification. Any Entity that maintains or possesses records or data containing PI of residents of MO that the Entity does not own or license, or any Entity that conducts business in MO that maintains or possesses records or data containing PI of a resident of MO that the person does not own or license, shall notify the owner or licensee of the information of any breach of security immediately following discovery of the breach, consistent with the legitimate needs of law enforcement as provided in this section.

Timing of Notification. The disclosure notification shall be made without unreasonable delay and consistent with any measures necessary to determine sufficient contact information and to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.

Personal Information Definition. An individual's first name or first initial and last name in combination with any one or more of the following data elements that relate to the individual if any of the data elements are not encrypted, redacted, or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable or unusable:

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	• Social Security Number; • Driver license number or other unique identification number created or collected by a government body; • Account number or credit card number or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; • Unique electronic identifier or routing code, in combination with any required security code, access code, or password that would permit access to an individual's financial account; • Medical information (information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional); or • Health insurance information (an individual's health insurance policy number, subscriber identification number, or any unique identifier used by a health insurer to identify the individual). PI does not include information that is lawfully obtained from publicly available sources, or from federal, state, or local government records lawfully made available to the general public. **Notice Required.** Notice may be provided by one of the following methods: • Written notice; • Telephonic notice, if such contact is made directly with the affected consumers; or • Electronic notice for those consumers for whom the person has a valid e-mail address and who have agreed to receive communications electronically, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 (E-SIGN Act). The notice shall at minimum include a description of the following: • The incident in general terms; • The type of PI that was obtained as a result of the breach of security; • A telephone number that the affected consumer may call for further information and assistance, if one exists; • Contact information for consumer reporting agencies; and • Advice that directs the affected consumer to remain vigilant by reviewing account statements and monitoring free credit reports. **Substitute Notice Available.** If the Entity demonstrates that the cost of providing notice would exceed $100,000, or that the class of affected consumers to be notified exceeds 150,000, or that the Entity does not have sufficient contact information or consent, for only those affected consumers without sufficient contact information or consent, or that the Entity is unable to identify particular affected consumers, for only those unidentifiable consumers. Substitute notice shall consist of all the following: • E-mail notice when the Entity has an electronic mail address for the affected consumer; • Conspicuous posting of the notice or a link to the notice on the Entity's Web site if the Entity maintains one; and

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	• Notification to major statewide media. **Exception: Own Notification Policy.** An Entity that maintains its own notice procedures as part of an information security policy for the treatment of PI, and whose procedures are otherwise consistent with the timing requirements of this section, is deemed to be in compliance with the notice requirements of this section if the Entity notifies affected consumers in accordance with its policies in the event of a breach of security of the system. **Exception: Compliance with Other Laws.** • An Entity that is regulated by state or federal law and that maintains procedures for a breach of the security of the system pursuant to the laws, rules, regulations, guidance, or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance with this section if the Entity notifies affected consumers in accordance with the maintained procedures when a breach occurs. • A financial institution that is: (i) subject to and in compliance with the Federal Interagency Guidance Response Programs for Unauthorized Access to Customer Information and Customer Notice, issued on March 29, 2005, by the board of governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision, and any revisions, additions, or substitutions relating to said interagency guidance; or (ii) subject to and in compliance with the National Credit Union Administration regulations in 12 C.F.R. Part 748; or (iii) subject to and in compliance with the provisions of Title V of the Gramm-Leach-Bliley Act shall be deemed to be in compliance with this section. **Penalties/Enforcement.** The state AG shall have exclusive authority to bring an action to obtain actual damages for a willful and knowing violation of this section and may seek a civil penalty not to exceed $150,000 per breach of the security of the system or series of breaches of a similar nature that are discovered in a single investigation. **Other Key Provisions:** • **Delay for Law Enforcement.** The notice required by this section may be delayed if a law enforcement agency informs the Entity that notification may impede a criminal investigation or jeopardize national or homeland security, provided that such request by law enforcement is made in writing or the Entity documents such request contemporaneously in writing, including the name of the law enforcement officer making the request and the officer's law enforcement agency engaged in the investigation. The notice required by this section shall be provided without unreasonable delay after the law enforcement agency communicates to the Entity its determination that notice will no longer impede the investigation or jeopardize national or homeland security.

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

Montana

Mont. Code § 30-14-1701 *et seq*.

H.B. 732 (signed into law April 28, 2005, Chapter 518)

Effective March 1, 2006

H.B. 74 (signed into law Feb. 27, 2015)

Effective October 1, 2015

[back to table of contents]

Application. Any person or business (collectively, Entity) that conducts business in MT and that owns or licenses computerized data that includes PI.

- The provisions governing maintenance of PI that the Entity does not own appear applicable to any Entity maintaining information on MT residents, whether or not the Entity conducts business in MT.

Security Breach Definition. Any unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of PI maintained by the Entity and causes or is reasonably believed to cause loss or injury to a MT resident.

- Good-faith acquisition of PI by an employee or agent of the Entity for the purpose of the Entity is not a breach of the security of the data system, provided that the PI is not used or subject to further unauthorized disclosure.

Notification Obligation. Any Entity to which the statute applies shall disclose any breach of the security of the data system following discovery or notification of the breach to any resident of MT whose unencrypted PI was or is reasonably believed to have been acquired by an unauthorized person.

Notification of Consumer Reporting Agencies. If a business notifies an individual of a breach and suggests, indicates or implies that the individual may obtain a credit report, the business must coordinate with the credit reporting agency as to the timing, content and distribution of notice to the individual (but this may not unreasonably delay disclosure of the breach).

[Effective October 1, 2015] Attorney General/Insurance Commissioner Notification. Any Entity that is required to issue a notification shall simultaneously submit an electronic copy of the notification and a statement providing the date and method of distribution of the notification to the attorney general's consumer protection office, excluding any information that personally identifies any individual who is entitled to receive notification. If a notification is made to more than one individual, a single copy of the notification must be submitted that indicates the number of individuals in the state who received notification.

Insurance entities and support organizations must submit the above information to the Montana Insurance Commissioner. Mont. Code § 33-19-321

Third-Party Data Notification. Any Entity that maintains computerized data that includes PI that the Entity does not own shall notify the owner or licensee of the information of any breach of the security of the data system immediately following discovery if the PI was or is reasonably believed to have been acquired by an unauthorized person.

Timing of Notification. Disclosure is to be made without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

Personal Information Definition.

An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

- social security number;
- driver's license number, state identification card number, or tribal identification card number;

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	• account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; [Effective October 1, 2015:] • medical record information as defined in 33-19-104 (Personal information that: (a) relates to an individual's physical or mental condition, medical history, medical claims history, or medical treatment; and (b) is obtained from a medical professional or medical care institution, from the individual, or from the individual's spouse, parent, or legal guardian.); • taxpayer identification number; or • an identity protection personal identification number issued by the U.S. Internal Revenue Service PI does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. **Notice Required.** Notice may be provided by one of the following methods: • Written notice; • Telephonic notice; or • Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 (E-SIGN Act). **Substitute Notice Available.** If the Entity demonstrates that the cost of providing notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000, or the Entity does not have sufficient contact information. Substitute notice shall consist of email notice when the Entity has an email address for the subject persons and one of the following: • Conspicuous posting of the notice on the Entity's Web site if the Entity maintains one; -or • Notification to applicable local or statewide media. **Exception: Own Notification Policy.** An Entity that maintains its own notification procedures as part of an information security policy for the treatment of PI and that does not unreasonably delay notice is considered to be in compliance with the notification requirements of the statute if the Entity notifies subject persons in accordance with its policies in the event of a breach of security of the data system. **Other Key Provisions:** • **Delay for Law Enforcement.** Notice may be delayed if a law enforcement agency determines that it will impede a criminal investigation and requests a delay in notification. The notification must be made after law enforcement agency determines that it will not compromise the investigation.

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

Nebraska

Neb. Rev. Stat. § 87-801 *et seq.*

L.B. 876 (signed into law April 10, 2006)

Effective July 14, 2006

L.B. 835 (signed into law April 13, 2016)Effective July 20, 2016

[back to table of contents]

Application. An individual, government agency, corporation, business trust, estate, trust, partnership, limited partnership, limited liability partnership, limited liability company, association, organization, joint venture, government, governmental subdivision, agency, or instrumentality, or any other legal entity, whether for profit or not for profit (collectively, Entity), that conducts business in NE and that owns or licenses computerized data that includes PI about a resident of NE.

- The provisions governing maintenance of PI that the Entity does not own appear applicable to any Entity maintaining information on NE residents, whether or not the Entity conducts business in NE.

Security Breach Definition. An unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of PI maintained by an Entity.

- Good-faith acquisition of PI by an employee or agent of an Entity for the purposes of the Entity is not a breach of the security of the system if the PI is not used or subject to further unauthorized disclosure.
- Acquisition of PI pursuant to a search warrant, subpoena, or other court order or pursuant to a subpoena or order of a state agency is not a breach of the security of the system.

Notification Obligation. Any Entity to which the statute applies shall, when it becomes aware of a breach of the security of the system and determines that the use of information about a NE resident for an unauthorized purpose has occurred or is reasonably likely to occur, give notice to the affected NE resident.

- Notification is not required if after a good-faith, reasonable and prompt investigation the Entity determines that it is unlikely that PI has been or will be used for an unauthorized purpose.

Attorney General/Regulator Notification. [Effective July 20, 2016: If notice of a security breach to Nebraska residents is required, the Entity shall also, not later than the time when notice is provided to the Nebraska resident, provide notice of the breach of security of the system to the Attorney General.**]**

Third-Party Data Notification. An Entity that maintains computerized data that includes PI that the Entity does not own or license shall give notice to and cooperate with the owner or licensee of the information of any breach of the security of the system when it becomes aware of a breach if use of PI about a NE resident for an unauthorized purpose occurred or is reasonably likely to occur. Cooperation includes, but is not limited to, sharing with the owner or licensee information relevant to the breach, not including information proprietary to the Entity.

Timing of Notification. Notice shall be made as soon as possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.

Personal Information Definition. Personal information means either of the following:

(a) A NE resident's first name or first initial and last name in combination with any one or more of the following data elements that relate to the resident if either the name or the data elements are not encrypted, redacted, or

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	otherwise altered by any method or technology in such a manner that the name or data elements are unreadable: • Social Security Number; • Driver license number or state identification card number; • Account number or credit card number or debit card number in combination with any required security code, access code, or password that would permit access to a resident's financial account; • Unique electronic ID number or routing code, in combination with any required security code, access code, or password; or • Unique biometric data, such as a fingerprint, voice print, or retina or iris image, or other unique physical representation; or (b) **[Effective July 20, 2016**: A user name or email address, in combination with a password or security question and answer, that would permit access to an online account.**]** **[Effective July 20, 2016:** Data shall not be considered encrypted if the confidential process or key was or is reasonably believed to have been acquired as a result of the breach of the security of the system**]** PI does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. **Notice Required.** Notice may be provided by one of the following methods: • Written notice; • Telephonic notice; or • Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 (E-SIGN Act). **Substitute Notice Available.** If the Entity demonstrates that the cost of providing notice will exceed $75,000, that the affected class of NE residents to be notified exceeds 100,000 residents, or that the Entity does not have sufficient contact information to provide notice. Substitute notice requires all of the following: • Email notice if the Entity has email addresses for the members of the affected class of NE residents; • Conspicuous posting of the notice on the Entity's Web site if it maintains one; and • Notice to major statewide media. **Substitute Notice Exception.** If the Entity has 10 employees or fewer and demonstrates that the cost of providing notice will exceed $10,000. Substitute notice requires all of the following: • Email notice if the Entity has email addresses for the members of the affected class of NE residents; • Notification by a paid advertisement in a local newspaper that is distributed in the geographic area in which the Entity is located, which advertisement shall be of sufficient size that it covers at least one-quarter of a page in the newspaper and shall be published in the newspaper at least once a week for three consecutive weeks;

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	• Conspicuous posting of the notice on the Entity's Web site if it maintains one; and • Notification to major media outlets in the geographic area in which the Entity is located. **Exception: Own Notification Policy.** An Entity that maintains its own notice procedures which are part of an information security policy for the treatment of PI and which are otherwise consistent with the timing requirements of the statute, is deemed to be in compliance with the notice requirements of the statute if the Entity notifies affected NE residents and Attorney General in accordance with its notice procedures in the event of a breach of the security of the system. **Exception: Compliance with Other Laws.** • **Primary Regulator.** An Entity that is regulated by state or federal law and that maintains procedures for a breach of the security of the system pursuant to the laws, rules, regulations, guidance, or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance with the notice requirements of the statute if the Entity notifies affected NE residents and Attorney General in accordance with the maintained procedures in the event of a breach of the security of the system. **Other Key Provisions:** • **Delay for Law Enforcement.** Notice may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation. Notice shall be made in good-faith, without unreasonable delay, and as soon as possible after the law enforcement agency determines that notification will no longer impede the investigation. • **AG Enforcement.** AG may issue subpoenas and seek and recover direct economic damages for each affected NE resident injured by a violation of the statute. • **Waiver Not Permitted.**

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

Nevada

Nev. Rev. Stat. § 603A.010 *et seq.*

S.B. 347 (signed into law June 17, 2005, Chapter 485)

Effective October 1, 2005: Provisions regarding (i) forgery laboratories, (ii) crimes against older and vulnerable persons, (iii) requirements for state actors, and (iv) credit card issuer requirements

Effective January 1, 2006: (i) credit card issuer requirements, (ii) data destruction requirements, (iii) "reasonable protections" requirements, (iv) security breach notification provisions

Effective January 1, 2008: Encryption provisions

S.B. No. 186 (signed into law June 15, 2011)

Effective October 1, 2011

A.B. 179 (Signed into law May 13, 2015)

Effective July 1, 2015

[back to table of contents]

Application. Any governmental agency, institution of higher education, corporation, financial institution or retail operator, or any other type of business entity or association (collectively, Entity), that owns or licenses computerized data that includes PI.

Security Breach Definition. An unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of PI maintained by Entity.

- Good-faith acquisition of PI by an employee or agent of the Entity for the legitimate purposes of the Entity is not a breach of the security of the system if the PI is not otherwise used or subject to further unauthorized disclosure.

Notification Obligation. Any Entity to which the statute applies shall disclose any breach of the security of the system data following discovery or notification of the breach to any resident of NV whose unencrypted PI was, or is reasonably believed to have been, acquired by an unauthorized person.

Notification to Consumer Reporting Agencies. If an Entity determines that notification is required to be given to more than 1,000 persons at any one time, the Entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the time the notification is distributed and the content of the notification.

Third-Party Data Notification. If an 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 the security of the system data immediately following discovery if the PI was, or is reasonably believed to have been, acquired by an unauthorized person.

Timing of Notification. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system data.

Personal Information Definition. An individual'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:

- Social Security Number;
- Driver license number, driver authorization card number or identification card number; or
- Account number or credit card number or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.

[Legislation effective July 1, 2015, but businesses exempted from compliance until July 1, 2016:]

- A medical identification number or a health insurance identification number.
- A user name, unique identifier or electronic mail address in combination with a password, access code or security question and answer that would permit access to an online account.

PI does not include the last four digits of a Social Security Number, the last four digits of a driver authorization card number, or the last four digits of an identification card number or publicly available information that is lawfully

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

made available to the general public from federal, state or local governmental records.

Notice Required. Notice may be provided by one of the following methods:

- Written notice; or
- Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 (E-SIGN Act).

Substitute Notice Available. If the Entity demonstrates that the cost of providing notice would exceed $250,000, the affected class of subject persons to be notified exceeds 500,000, or the Entity does not have sufficient contact information. Substitute notice shall consist of all of the following:

- Email notice when the Entity has an email addresses for the subject persons;
- Conspicuous posting of the notice on the Entity's Web site if the Entity maintains one; and
- Notification to major statewide media.

Exception: Own Notification Policy. An Entity that maintains its own notification policies and procedures as part of an information security policy for the treatment of PI that is otherwise consistent with the timing requirements of the statute shall be deemed in compliance with the notification requirements of the statute if it notifies subject persons in accordance with its policies and procedures in the event of a security breach.

Exception: Compliance with Other Laws.

- **Gramm-Leach-Bliley Act.** An Entity that is subject to and complies with the privacy and security provisions of the Gramm-Leach-Bliley Act shall be deemed to be in compliance with the notification requirements.

Other Key Provisions:

- **Delay for Law Enforcement.** The notification required by the statute may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification must be made after the law enforcement agency determines that the notification will not compromise the investigation.
- **AG Enforcement.** If the state AG or a district attorney of any county has reason to believe that any person is violating, proposes to violate or has violated the provisions of the statute, he may bring an action against that person to obtain a temporary or permanent injunction against the violation.
- **Right of Action for Data Collector.** A data collector that provides the requisite notice may commence an action for damages against a person that unlawfully obtained or benefited from personal information obtained from records maintained by the data collector.
- **Special Notification Obligations for Government Agencies and Elected Officers.** *See* Nev. Rev. Stat. § 242.181.

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	• **Special Rules Applicable to Electronic Health Records.** *See* Nev. Rev. Stat. §§ 439, 603A.100. • **Waiver Not Permitted.**

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

New Hampshire

N.H. Rev. Stat. § 359-C:19 *et seq*.

H.B. 1660 (signed into law June 2, 2006)

Effective January 1, 2007

[back to table of contents]

Application. Any individual, corporation, trust, partnership, incorporated or unincorporated association, limited liability company, or other form of entity, or any agency, authority, board, court, department, division, commission, institution, bureau, or other state governmental entity, or any political subdivision of the state (collectively, Entity) doing business in NH that owns or licenses computerized data that includes PI.

- The provisions governing maintenance of PI that the Entity does not own appear applicable to any Entity maintaining PI, whether or not the Entity does business in NH.

Security Breach Definition. An unauthorized acquisition of computerized data that compromises the security or confidentiality of PI maintained by an Entity doing business in NH.

- Good-faith acquisition of PI by an employee or agent of an Entity for the purposes of the Entity's business shall not be considered a security breach, provided that the PI is not used or subject to further unauthorized disclosure.

Notification Obligation. Any Entity to which the statute applies, when it becomes aware of a security breach and determines that misuse of the information has occurred or is reasonably likely to occur, or if a determination cannot be made, shall notify the affected individuals.

- Notification is not required if it is determined that misuse of the information has not occurred and is not reasonably likely to occur.

Notification to Consumer Reporting Agencies. If an Entity is required to notify more than 1,000 consumers, the Entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the anticipated date of the notification, the approximate number of consumers who will be notified, and the content of the notice. This obligation does not apply to entities subject to Title V of the Gramm-Leach-Bliley Act.

Attorney General/Regulator Notification. An Entity engaged in trade or commerce that is subject to N.H. Rev. Stat. § 358-A:3(I) (trade or commerce that is subject to the jurisdiction of the bank commissioner, the director of securities regulation, the insurance commissioner, the public utilities commission, the financial institutions and insurance regulators of other states, or federal banking or securities regulators who possess the authority to regulate unfair or deceptive trade practices) shall also notify the regulator which has primary regulatory authority over such trade or commerce. All other Entities shall notify the state AG. The notice shall include the anticipated date of the notice to the individuals and the approximate number of individuals in NH who will be notified.

Third-Party Data Notification. If an Entity maintains computerized data that includes PI that the Entity does not own, the Entity shall notify and cooperate with the owner or licensee of the information of any breach of the security of the data immediately following discovery if the PI was acquired by an unauthorized person. 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 or business information or trade secrets.

Timing of Notification. The Entity shall notify the affected individuals as soon as possible.

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	Personal Information Definition. An individual's first name or initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: • Social Security Number; • Driver license number or other government identification number; or • Account number or credit card number or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account. 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. PI shall not include information that is lawfully made available to the general public from federal, state, or local government records. **Notice Required.** Notice shall include at a minimum: • A description of the incident in general terms; • The approximate date of the breach; • The type of PI obtained as a result of the security breach; and • The telephonic contact information of the Entity. Notice shall be provided by one of the following methods: • Written notice; • Telephonic notice, provided that a log of each such notification is kept by the person or business who notifies affected persons; • Electronic notice, if the Entity's primary means of communication with affected individuals is by electronic means; or • Notice pursuant to the Entity's internal notification procedures maintained as part of an information security policy for the treatment of PI. **Substitute Notice Available.** If the Entity demonstrates that the cost of providing notice would exceed $5,000, the affected class of subject individuals to be notified exceeds 1,000, or the Entity does not have sufficient contact information or consent to provide written, electronic or telephonic notice. Substitute notice shall consist of all of the following: • Email notice when the Entity has an email address for the affected individuals; • Conspicuous posting of the notice on the Entity's Web site if the Entity maintains one; and • Notification to major statewide media. **Exception: Compliance with Other Laws.** • **Primary Regulator.** An Entity engaged in trade or commerce that maintains procedures for security breach notification pursuant to laws, rules, regulations, guidance, or guidelines issued by a state or federal regulator shall be deemed to be in compliance with this subdivision if it acts in accordance with such laws, rules, regulations, guidance or guidelines.

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	Other Key Provisions: • **Delay for Law Enforcement.** The notification may be delayed if a law enforcement agency or national or homeland security agency determines that the notification will impede a criminal investigation or jeopardize national or homeland security. • **AG Enforcement.** • **Private Right of Action.** Any person injured by any violation may bring a civil action. If the court finds for the plaintiff, recovery shall be in the amount of actual damages. If the court finds that the act or practice was willful or knowing, it shall award as much as three times but not less than two times, such amount. In addition, a prevailing plaintiff shall be awarded the costs of the suit and attorney's fees, as determined by the court. Injunctive relief shall be available to private individuals under this chapter without bond, subject to the discretion of the court. • **Waiver Not Permitted.**

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

New Jersey

N.J. Stat. § 56:8-163

A. 4001 (signed Sept. 22, 2005)

Effective January 1, 2006 (all provisions except those governing police reports, which are effective on Sept. 22, 2005)

[back to table of contents]

Application. NJ, and any county, municipality, district, public authority, public agency, and any other political subdivision or public body in NJ, any sole proprietorship, partnership, corporation, association, or other entity, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the law of NJ, any other state, the United States, or of any other country, or the parent or the subsidiary of a financial institution, that conducts business in NJ (collectively, Entity) that compiles or maintains computerized records that include PI.

- The provisions governing maintenance of PI that the Entity does not own appear applicable to any Entity maintaining PI, whether or not the Entity conducts business in NJ.

Security Breach Definition. 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 or technology that renders the PI unreadable or unusable.

- Good-faith acquisition of PI by an employee or agent of the Entity for a legitimate business purpose is not a breach of security, provided that the PI is not used for a purpose unrelated to the business or subject to further unauthorized disclosure.

Notification Obligation. Any Entity to which the statute applies shall disclose any breach of security of computerized records following discovery or notification of the breach to any customer who is a resident of NJ whose PI was, or is reasonably believed to have been, accessed by an unauthorized person.

- Disclosure of a breach of security to a customer shall not be required if the Entity establishes that misuse of the information is not reasonably possible. Any determination shall be documented in writing and retained for five years.

Notification to Consumer Reporting Agencies. If an Entity discovers circumstances requiring notification pursuant to this section of more than 1,000 persons at one time, the Entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile or maintain files on consumers on a nationwide basis of the timing, distribution and content of the notices.

Attorney General/Police Notification. Any Entity required under this section to disclose a breach of security of a customer's PI shall, prior to disclosure to the customer, report the breach of security and any information pertaining to the breach to the Division of State Police in the Department of Law and Public Safety for investigation or handling, which may include dissemination or referral to other appropriate law enforcement entities.

Third-Party Data Notification. An Entity that compiles or maintains computerized records that include PI on behalf of another Entity shall notify that Entity of any breach of security of the computerized records immediately following discovery, if the PI was, or is reasonably believed to have been, accessed by an unauthorized person.

Timing of Notification. The disclosure to a customer shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

Personal Information Definition. An individual's first name or first initial and

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	last name linked with any one or more of the following data elements: • Social Security Number; • Driver license number or state identification card number; or • Account number or credit card number or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account. Dissociated data that, if linked, would constitute PI is PI if the means to link the dissociated data were accessed in connection with access to the dissociated data. PI shall not include publicly available information that is lawfully made available to the general public from federal, state or local government records, or widely distributed media. **Notice Required.** Notice may be provided by one of the following methods: • Written notice; or • Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 (E-SIGN Act). **Substitute Notice Available.** If the Entity demonstrates that the cost of providing notice would exceed $250,000, or that the affected class of subject individuals to be notified exceeds 500,000, or the Entity does not have sufficient contact information. Substitute notice shall consist of all of the following: • Email notice when the Entity has email addresses; • Conspicuous posting of the notice on the Entity's Web site if the Entity maintains one; and • Notification to major statewide media. **Exception: Own Notification Policy.** An Entity that maintains its own notification procedures as part of an information security policy for the treatment of PI, and is otherwise consistent with the requirements of the statute, shall be deemed in compliance with the notification requirements of the statute if it notifies subject customers in accordance with its policies in the event of a breach of security of the system. **Other Key Provisions:** • **Delay for Law Enforcement.** The notification required by this section shall be delayed if a law enforcement agency determines that the notification will impede a criminal or civil investigation and that agency has made a request that the notification be delayed.

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

New York

N.Y. Gen. Bus. Law § 899-aa

A.B. 4254 (signed into law August 10, 2005)

N.Y. State Tech. Law § 208

Effective December 7, 2005

S. 2605-D (signed into law March 28, 2013)

Effective March 28, 2013

[back to table of contents]

Application. Any person, business, or state entity (excepting the judiciary, cities, counties, municipalities, villages, towns and other local agencies) (collectively, Entity) which conducts business in New York state and which owns or licenses computerized data which includes private information.

- The provisions governing maintenance of private information that the Entity does not own appear applicable to any Entity maintaining private information, whether or not the Entity conducts business in NY.

Security Breach Definition. Unauthorized acquisition or acquisition without valid authorization of computerized data that compromises the security, confidentiality, or integrity of PI maintained by a business. In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization, Entities may consider the following factors, among others:

- 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;
- Indications that the information has been downloaded or copied; or
- Indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

Good-faith acquisition of PI by an employee or agent of the Entity for the purposes of the Entity is not a breach of the security of the system, provided that the private information is not used or subject to unauthorized disclosure.

Notification Obligation. Any Entity to which the statute applies shall disclose any breach of the security following discovery or notification of the breach in the security of the system to any resident of NY whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization.

Notification to Consumer Reporting Agencies. If more than 5,000 NY residents are to be notified at one time, the Entity shall also notify consumer reporting agencies as to the timing, content and distribution of the notices and approximate number of affected persons.

Attorney General/Agency Notification. If any NY residents are to be notified, the Entity shall notify the state Attorney General, the consumer protection board, the division of state police, and the state Office of Information Technology Services as to the timing, content and distribution of the notices and approximate number of affected persons. The state AG's website has a form to be used for notifications.

Third-Party Data Notification. Any Entity that maintains computerized data that includes private information that the Entity does not own shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the private information was, or is reasonably believed to have been, acquired by a person without valid authorization.

Timing of Notification. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system.

Personal Information Definition. Information concerning a natural person

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	which, because of name, number, personal mark, or other identifier, can be used to identify such natural person **Private Information Definition.** Personal information consisting of any information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted, or encrypted with an encryption key that has also been acquired: • Social Security Number; • Driver license number or non-driver identification card number; or • Account number or credit card number or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account. "Private information" does not include publicly available information which is lawfully made available to the general public from federal, state, or local government records. **Notice Required.** Notice shall include: • Contact information for the Entity making the notification; and • A description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which of the elements of PI and private information were, or are reasonably believed to have been, so acquired. The notice required shall be directly provided to the affected persons by one of the following methods: • Written notice; • Telephonic notice, provided that a log of each such notification is kept by the Entity; or • Electronic notice, provided that the person to whom notice is required has expressly consented to receiving said notice in electronic form and a log of each such notification is kept by the Entity who notifies affected persons in such form; provided further, however, that in no case shall any Entity require a person to consent to accepting said notice in said form as a condition of establishing any business relationship or engaging in any transaction. **Substitute Notice Available.** If the Entity demonstrates to the state AG that the cost of providing notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000, or the Entity does not have sufficient contact information. Substitute notice shall consist of <u>all</u> of the following: • Email notice when the Entity has an email addresses for the subject persons; • Conspicuous posting of the notice on the Entity's Web site if the Entity maintains one; and • Notification to major statewide media. **Other Key Provisions:** • **Delay for Law Enforcement.** The notification required by this

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	section may be delayed if a law enforcement agency determines that such notification impedes a criminal investigation. The required notification shall be made after such law enforcement agency determines that such notification does not compromise such investigation. • **AG Enforcement.** The AG may bring an action to enjoin and restrain the continuation of such violation.

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

North Carolina

N.C. GEN. STAT. §§ 75-61, 75-65

Effective December 1, 2005

S.B. 1048 (signed into law September 21, 2005)

Amended by S.B. 1017 (signed into law July 27, 2009)

[back to table of contents]

Application. Any sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the laws of any state or country, or the parent or the subsidiary of any such financial institution, but not including any government or governmental subdivision or agency (collectively, Entity) that owns or licenses PI of residents of NC or any Entity that conducts business in NC that owns or licenses PI in any form (computerized, paper, or otherwise).

Security Breach Definition. 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. Any incident of unauthorized access to and acquisition of encrypted records or data containing PI along with the confidential process or key shall constitute a security breach.

- Good-faith acquisition of PI by an employee or agent of the Entity for a legitimate purpose is not a security breach, provided that the PI is not used for a purpose other than a lawful purpose of the Entity and is not subject to further unauthorized disclosure.

Notification Obligation. Any Entity to which the statute applies shall provide notice to the affected person that there has been a security breach following discovery or notification of the breach.

Notification to Consumer Reporting Agencies. In the event an Entity provides notice to more than 1,000 persons at one time pursuant to this section, the Entity shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution, and content of the notice.

Attorney General Notification. In the event a business provides notice to an affected person pursuant to this section, the business shall notify without unreasonable delay the Consumer Protection Division of the state AG's office of the nature of the breach, the number 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. The AG's website contains a form to be used for notification.

Third-Party Data Notification. Any business that possesses records containing PI of residents of NC that the business does not own or license, or conducts business in NC that possesses records containing PI that the business does not own or license shall notify the owner or licensee of the information of any security breach immediately following discovery of the breach.

Timing of Notification. The disclosure shall be made without unreasonable delay, consistent with any measures necessary to determine sufficient contact information, determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.

Personal Information Definition. A person's first name or first initial and last name in combination with any of the following identifying information:

- Social Security Number or employer taxpayer identification numbers;
- Drivers license, state identification card or passport numbers;
- Checking account numbers;

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	• Savings account numbers; • Credit card numbers; • Debit card numbers; • PIN; • Digital signatures; • Any other numbers or information that can be used to access a person's financial resources; • Biometric data; or • Fingerprints. Additionally, if (but only if) any of the following information "would permit access to a person's financial account or resources," it is considered PI when taken in conjunction with a person's first name, or first initial and last name: • Electronic ID numbers; • Email names or addresses; • Internet account numbers; • Internet ID names; • Parent's legal surname prior to marriage; or • Passwords. PI does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, including name, address, and telephone number, and does not include information made lawfully available to the general public from federal, state, or local government records **Notice Required.** Notice must be clear, conspicuous, and shall include all of the following: • A description of the incident in general terms; • A description of the type of PI that was subject to the unauthorized access and acquisition; • A description of the general acts of the business to protect the PI from further unauthorized access; • A telephone number for the business that the person may call for further information and assistance, if one exists; • Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports; • The toll-free numbers and addresses for the major consumer reporting agencies; and • The toll-free numbers, addresses, and Web site 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 preventing identity theft. It may be provided by one of the following methods: • Written notice; • Telephonic notice provided that contact is made directly with the affected persons; or • Electronic notice, for those persons for whom it has a valid e-mail address and who have agreed to receive communications

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	electronically if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 (E-SIGN Act). **Substitute Notice Available.** If the business demonstrates that the cost of providing notice would exceed $250,000 or that the affected class of subject persons to be notified exceeds 500,000, or if the business does not have sufficient contact information or consent to provide notice as required under the statute, for only those affected persons without sufficient contact information or consent, or if the business is unable to identify particular affected persons, for only those unidentifiable affected persons. Substitute notice shall consist of all the following: • Email notice when the Entity has an email address for the subject persons; • Conspicuous posting of the notice on the Entity's Web site if the Entity maintains one; and • Notification to major statewide media. **Exception: Compliance with Other Laws.** • A financial institution that is subject to and in compliance with the Federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice, issued on March 7, 2005, by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision, and any revisions, additions, or substitutions relating to said Interagency Guidance, shall be deemed to be in compliance. **Other Key Provisions:** • **Delay for Law Enforcement.** The notice required by this section shall be delayed if a law enforcement agency informs the business that notification may impede a criminal investigation or jeopardize national or homeland security, provided that such request is made in writing or the business documents such request contemporaneously in writing, including the name of the law enforcement officer making the request and the officer's law enforcement agency engaged in the investigation. The notice required shall be provided without unreasonable delay after the law enforcement agency communicates to the business its determination that notice will no longer impede the investigation or jeopardize national or homeland security. • **AG Enforcement.** Civil and criminal penalties available. • **Private Right of Action.** An individual injured as a result of a violation of this section may institute a civil action. • **Waiver Not Permitted.**

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

North Dakota

N.D. Cent. Code § 51-30-01 *et seq.*

S.B. 2251 (signed into law April 22, 2005)

Effective June 1, 2005

H.B. 1435 (signed into law April 18, 2013)

S.B. 2214 (signed into law April 13, 2015)

Effective August 1, 2015

[back to table of contents]

Application. Any Entity that conducts business in ND and that owns or licenses computerized data that includes PI.

- The provisions governing maintenance of PI that the Entity does not own appear applicable to any Entity maintaining PI, whether or not the Entity conducts business in ND.

Security Breach Definition. 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 data bases unreadable or unusable.

- Good-faith acquisition of PI by an employee or agent of the Entity is not a breach of the security of the system if the PI is not used or subject to further unauthorized disclosure.

Notification Obligation. Any Entity to which the statute applies shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of ND whose unencrypted PI was, or is reasonably believed to have been, acquired by an unauthorized person.

Attorney General Notification. [Effective August 1, 2015] Any person that experiences a breach of the security system shall disclose to the attorney general by mail or email any breach of the security system which exceeds two hundred fifty individuals.

Third-Party Data Notification. Any person that maintains computerized data that includes PI that the person does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following the discovery, if the PI was, or is reasonably believed to have been, acquired by an unauthorized person.

Timing of Notification. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and to restore the integrity of the data system.

Personal Information Definition. An individual's first name or first initial and last name in combination with any of the following data elements, when the name and the data elements are not encrypted:

- Social Security Number;
- The operator's license number assigned to an individual by the department of transportation;
- A non-driver color photo identification card number assigned to the individual by the department of transportation;
- Account number or credit card number or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial accounts;
- The individual's date of birth;
- The maiden name of the individual's mother;
- Medical information;
- Health insurance information;
- An identification number assigned to the individual by the individual's employer in combination with any required security code, access code, or password; or

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	• The individual's digitized or other electronic signature. PI does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. **Notice Required.** Notice may be provided by one of the following methods: • Written notice; or • Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 (E-SIGN Act). **Substitute Notice Available.** If the person demonstrates that the cost of providing notice would exceed $250,000, the affected class of subject individuals to be notified exceeds 500,000, or the person does not have sufficient contact information. Substitute notice shall consist of all of the following: • Email notice when the person has an email address for the subject persons; • Conspicuous posting of the notice on the Entity's Web site if the Entity maintains one; and • Notification to major statewide media. **Exception: Own Notification Policy.** An Entity that maintains its own notification procedures as part of an information security policy for the treatment of PI and is otherwise consistent with the timing requirements of this chapter is deemed to be in compliance with the notification requirements of this chapter if the Entity notifies subject individuals in accordance with its policies in the event of a breach of security of the system. **Exception: Compliance with Other Laws.** • A financial institution, trust company, or credit union that is subject to, examined for, and in compliance with the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice is deemed to be in compliance with this chapter. • An Entity, business associate, or subcontractor that is subject to the breach notification requirements of title 45 of the Code of Federal Regulations, part 164, subpart D, is considered to be in compliance with this chapter. **Other Key Provisions:** • **Delay for Law Enforcement.** The notification required by this chapter may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The required notification must be made after the law enforcement agency determines that the notification will not compromise the investigation. • **AG Enforcement.**

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

Ohio

Ohio Rev. Code § 1349.19

H.B. 104 (signed into law Nov. 17, 2005), amended by S.B. 126 (signed into law Dec. 29, 2006)

Effective February 17, 2006 (amendment to exclude "covered entities" under HIPAA effective March 30, 2007)

[back to table of contents]

Application. Any individual, corporation, business trust, estate, trust, partnership, or association (collectively, Entity) that conducts business in OH and owns or licenses computerized data that includes PI.

- The provisions governing maintenance of PI that the Entity does not own appear applicable to any Entity maintaining PI, whether or not the Entity conducts business in OH.

Security Breach Definition. Unauthorized access to and acquisition of computerized data that compromises the security or confidentiality of PI owned or licensed by an Entity and that causes, reasonably is believed to have caused, or reasonably is believed will cause a material risk of identity theft or other fraud to the person or property of OH.

Notification Obligation. Any Entity to which the statute applies shall disclose any breach of the security of the system, following its discovery or notification of the breach of the security of the system, to any individual whose principal mailing address as reflected in the records of the Entity is in OH and whose PI was, or reasonably is believed to have been, accessed and acquired by an unauthorized person if the access and acquisition by the unauthorized person causes or reasonably is believed will cause a material risk of identity theft or other fraud to the resident.

Notification to Consumer Reporting Agencies. If an Entity discovers circumstances that require disclosure under this section to more than 1,000 residents of OH involved in a single occurrence of a breach of the security of the system, the Entity shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution, and content of the disclosure given by the Entity to the residents of OH. This requirement does not apply to "covered entities" as defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Third-Party Data Notification. Any Entity that, on behalf of or at the direction of another Entity or on behalf of or at the direction of any governmental entity, is the custodian of or stores computerized data that includes PI shall notify that other Entity or governmental entity of any breach of the security of the system in an expeditious manner, if the PI was, or reasonably is believed to have been, accessed and acquired by an unauthorized person and if the access and acquisition by the unauthorized person causes or reasonably is believed will cause a material risk of identity theft or other fraud to a resident of OH.

Timing of Notification. The disclosure shall be made in the most expedient time possible but not later than 45 days following discovery or notification of the breach in the security of the system, consistent with any measures necessary to determine the scope of the breach, including which residents' PI was accessed and acquired, and to restore the reasonable integrity of the data system.

Personal Information Definition. An individual's name, consisting of the individual's first name or first initial and last name, in combination with and linked to any one or more of the following data elements, when the data elements are not encrypted, redacted, or altered by any method or technology in such a manner that the data elements are unreadable:

- Social Security Number;
- Driver license number or state identification card number; or
- Account number or credit card number or debit card number in

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

combination with and linked to any required security code, access code, or password that would permit access to an individual's financial account.

PI does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or any of the following that are widely distributed:

- Any news, editorial, or advertising statement published in any bona fide newspaper, journal, or magazine, or broadcast over radio or television, or any type of media similar in nature;
- Any gathering or furnishing of information or news by any bona fide reporter, correspondent, or news bureau to any bona fide newspaper, journal, magazine, radio or television news media, or any type of media similar in nature; or
- Any publication designed for and distributed to members of any bona fide association or charitable or fraternal nonprofit corporation, or any type of media similar in nature.

Notice Required. Notice may be provided by any of the following methods:

- Written notice;
- Telephonic notice; or
- Electronic notice, if the Entity's primary method of communication with the resident to whom the disclosure must be made is by electronic means.

Substitute Notice Available. If the Entity demonstrates that the cost of providing disclosure or notice to residents to whom disclosure or notification is required would exceed $250,000, that the affected class of subject residents to whom disclosure or notification is required exceeds 500,000 persons, or that it does not have sufficient contact information to provide written, telephonic or electronic notice. Substitute notice under this division shall consist of all of the following:

- Email notice if the Entity has an email address for the resident to whom the disclosure must be made;
- Conspicuous posting of the notice on the Entity's Web site if the Entity maintains one; and
- Notification to major media outlets, to the extent that the cumulative total of the readership, viewing audience, or listening audience of all of the outlets so notified equals or exceeds 75% of the population of OH.

Substitute Notice Exception. If the Entity demonstrates it has 10 employees or fewer and that the cost of providing the disclosures or notices to residents to whom disclosure or notification is required will exceed $10,000. Substitute notice under this division shall consist of all of the following:

- Notification by a paid advertisement in a local newspaper that is distributed in the geographic area in which the Entity is located, which advertisement shall be of sufficient size that it covers at least one-quarter of a page in the newspaper and shall be published in the newspaper at least once a week for three consecutive weeks;
- Conspicuous posting of the disclosure or notice on the Entity's

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	Web site if the Entity maintains one; and • Notification to major media outlets in the geographic area in which the Entity is located. **Exception: Compliance with Other Laws.** • A financial institution, trust company, or credit union or any affiliate of a financial institution, trust company, or credit union that is required by federal law, including, but not limited to, any federal statute, regulation, regulatory guidance, or other regulatory action, to notify its customers of an information security breach with respect to information about those customers and that is subject to examination by its functional government regulatory agency for compliance with the applicable federal law, is exempt from the requirements of the statute. **Exception: Preexisting Contract.** Disclosure may be made pursuant to any provision of a contract entered into by the Entity with another Entity prior to the date the breach of the security of the system occurred if that contract does not conflict with any provision of this section and does not waive any provision of this section. **Other Key Provisions:** • **Delay for Law Enforcement.** The Entity may delay the disclosure if a law enforcement agency determines that the disclosure or notification will impede a criminal investigation or jeopardize homeland or national security, in which case, the Entity shall make the disclosure or notification after the law enforcement agency determines that disclosure or notification will not compromise the investigation or jeopardize homeland or national security. • **AG Enforcement.** The AG may conduct an investigation and bring a civil action upon an alleged failure by an Entity to comply with this statute.

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

Oklahoma

24 Okla. Stat. § 161 *et seq*.

H.B. 2245 (signed into law April 28, 2008)

Effective November 1, 2008

[back to table of contents]

Application. Any 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 (collectively, Entity) that owns or licenses computerized data that includes PI of OK residents.

Security Breach Definition. Unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of PI maintained by an Entity as part of a database of PI regarding multiple individuals and that causes, or the Entity reasonably believes has caused or will cause, identity theft or other fraud to any resident of OK.

- Good-faith acquisition of PI by an employee or agent of an Entity for the purposes of the Entity is not a breach of the security of the system, provided that the PI is not used for a purpose other than a lawful purpose of the Entity or subject to further unauthorized disclosure.

Notification Obligation. Any Entity to which the statute applies shall disclose any breach of the security of the system following discovery or notification of the breach of the security of the system to any resident of OK whose unencrypted and unredacted PI was or is reasonably believed to have been accessed and acquired by an unauthorized person and that causes, or the individual or entity reasonably believes has caused or will cause, identity theft or other fraud to any resident of OK.

- An Entity must disclose the breach of the security of the system 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 OK.

Third-Party Data Notification. An Entity that maintains computerized data that includes PI that the Entity does not own or license shall notify the owner or licensee of the information of any breach of the security of the system as soon as practicable following discovery, if the PI was or if the Entity reasonably believes was accessed and acquired by an unauthorized person.

Timing of Notification. The disclosure shall be made without unreasonable delay consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the system.

Personal Information Definition. The first name or first initial and last name of an individual in combination with and linked to any one or more of the following data elements that relate to a resident of OK, when the data elements are neither encrypted nor redacted:

- Social Security Number;
- Driver license or state identification card number issued in lieu of a driver license; or
- Account number or credit card number or debit card number in combination with any required security code, access code, or password that would permit access to the financial accounts of a resident.

PI shall not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	available to the general public. **Notice Required.** Notice means one of the following methods: • Written notice to the postal address in the records of the Entity; • Telephonic notice; or • Electronic notice. **Substitute Notice Available.** If an Entity demonstrates that the cost of providing notice would exceed $50,000, the affected class of residents to be notified exceeds 100,000, or the Entity does not have sufficient contact information or consent to provide notice. Substitute notice consists of any two of the following: • Email notice if the Entity has e-mail addresses for the members of the affected class of residents; • Conspicuous posting of the notice on the Entity's Web site if the Entity maintains one; or • Notification to major statewide media. **Exception: Own Notification Policy.** An entity that maintains its own notification procedures as part of an information privacy or security policy for the treatment of PI and that are consistent with the timing requirements of the statute shall be deemed to be in compliance with the notification requirements of the statute if it notifies residents of OK in accordance with its procedures in the event of a breach of security of the system. **Exception: Compliance with Other Laws.** • **Interagency Guidance.** 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 in compliance with the provisions of the statute. • **Primary Regulator.** An Entity that complies with the notification requirements or procedures pursuant to the rules, regulation, procedures, or guidelines established by the primary or functional federal regulator of the Entity shall be deemed to be in compliance with the provisions of the statute. **Penalties.** The state AG or a district attorney shall have exclusive authority to bring an action and may obtain either actual damages for a violation of the statute or a civil penalty not to exceed $150,000 per breach of the security of the system or series of breaches of a similar nature that are discovered in a single investigation. **Other Key Provisions:** • **Delay for Law Enforcement.** Notice required may be delayed if a law enforcement agency determines and advises the Entity that the notice will impede a criminal or civil investigation or homeland or national security. Notice required must be made without unreasonable delay after the law enforcement agency determines that notification will no longer impede the investigation or jeopardize national or homeland security.

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

Oregon

Or. Rev. Stat. §§ 646A.600, 646A.602, 646A.604, 646A.624, 646A.626

S.B. 583 (signed into law July 12, 2007)

Effective October 1, 2007

S.B. 574 (signed into law June 13, 2013)

Effective Sept. 12, 2013

S.B. 601 (signed into law June 10, 2015)

Effective Jan. 1, 2016

[back to table of contents]

Application. Any individual, private or public corporation, partnership, cooperative, association, estate, limited liability company, organization or other entity, whether or not organized to operate at a profit, or a public body as defined in Or. Rev. Stat. § 174.109 (collectively, Entity) that owns or licenses PI that is used in the course of the Entity's business, vocation, occupation or volunteer activities and was subject to the breach of security.

Security Breach Definition. Unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of PI maintained by the Entity.

- Does not include an inadvertent acquisition of PI by an Entity or that Entity's employee or agent if the PI is not used in violation of applicable law or in a manner that harms or poses an actual threat to the security, confidentiality or integrity of the PI.

Notification Obligation. Any Entity to which the statute applies shall give notice of the breach of security following discovery of such breach of security, or receipt of notification, to any consumer to whom the PI pertains .

- Notification is not required if, after an appropriate investigation or after consultation with relevant federal, state or local agencies responsible for law enforcement, the Entity reasonably determines that the breach has not and will not likely result in harm to the individuals whose PI has been acquired and accessed. Such a determination must be documented in writing and the documentation must be maintained for five years.

Notification to Consumer Reporting Agencies. If an Entity discovers a breach of security affecting more than 1,000 individuals that requires disclosure under this section, the Entity shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain reports on individuals on a nationwide basis of the timing, distribution and content of the notification given by the Entity to the individuals. The Entity shall include the police report number, if available, in its notification to the consumer reporting agencies.

[Effective Jan 1, 2016: Attorney General Notification. The entity must provide notice to the Attorney General, either in writing or electronically, if the number of residents affected exceeds 250. The Entity shall disclose the breach of security to the Attorney General in the same manner as to consumers.**]**

Third-Party Data Notification. Any person that maintains or otherwise possesses PI on behalf of, or under license of, another person shall notify the other person of any breach of security immediately following discovery of such breach of security if an individual's PI was included in the information that was breached.

Timing of Notification. The disclosure shall be made in the most expedient manner possible and without unreasonable delay, consistent with any measures necessary to determine sufficient contact information for the individuals, determine the scope of the breach and restore the reasonable integrity, security and confidentiality of the PI.

Personal Information Definition. An OR resident's first name or first initial and last name in combination with any one or more of the following data elements, if encryption, redaction or other methods have not rendered the data unusable or if the data elements are encrypted and the encryption key has also been acquired:

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	• Social Security Number; • Driver license number or state identification card number issued by the department of transportation; • Passport number or other identification number issued by the United States; • Account number or credit card number or debit card number in combination with any required security code, access code, or password that would permit access to an OR resident's financial account. **[Effective Jan. 1, 2016:** • Biometric data from automatic measurements of a consumer's physical characteristics, such as an image of a fingerprint, retina or iris, that are used to authenticate the consumer's identity in the course of a financial or other transaction • a consumer's health insurance policy number or health insurance subscriber identification number in combination with any other unique identifier that a health insurer uses to identify the consumer • any information about a consumer's medical history or mental or physical condition or about a health care professional's medical diagnosis or treatment of the consumer**]** PI also includes any PI data element or any combination of the PI data elements without with the consumer's first name or first initial and last name if encryption, redaction, or other methods have not rendered the data element or combination of data elements unusable and the data element or combination of data elements would enable an individual to commit identity theft. PI does not include publicly available information, other than a Social Security Number, that is lawfully made available to the general public from federal, state or local government records. **Notice Required.** Notice shall include at a minimum: • A description of the breach of security in general terms; • The approximate date of the breach of security; • The type of PI that was subject to the breach of security; • Contact information for the person that owned or licensed the PI that was subject to the breach; • Contact information for national consumer reporting agencies; and • Advice to the individual to report suspected identity theft to law enforcement, including the Attorney General and the Federal Trade Commission. Notice may be provided by one of the following methods: • In writing; • By telephone, if the Entity contacts the affected consumer directly; or • Electronically, if the Entity's primary method of communication with the individual is by electronic means or is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 (E-SIGN Act).

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	Substitute Notice Available. If the Entity demonstrates that the cost of providing notice would exceed $250,000, that the affected class of individuals to be notified exceeds 350,000, or if the Entity does not have sufficient contact information to provide notice. Substitute notice consists of the following: • Conspicuous posting of the notice or a link to the notice on the Entity's Web site if the Entity maintains a website; and • Notification to major statewide television and newspaper media. **Exception: Compliance with Other Laws.** • **Primary Regulator.** An Entity that complies with the notification requirements or breach of security procedures that provide greater protection to PI and at least as thorough disclosure requirements pursuant to the rules, regulations, procedures, guidance or guidelines established by the Entity's primary or functional federal regulator. • **Gramm-Leach-Bliley Act.** A person that complies with regulations regarding notification requirements or breach of security procedures that provide greater protection to PI and at least as thorough disclosure requirements promulgated pursuant to Title V of the Gramm-Leach-Bliley Act. • **HIPAA.** An Entity covered by HIPAA if the Entity sends the Attorney General a copy of the notice that was sent to consumers under ORS 646A.604 or to the primary functional regulator designated for the covered entity under HIPAA. • **More Restrictive State or Federal Law.** An Entity that complies with a state or federal law that provides greater protection to PI and at least as thorough disclosure requirements for breach of security of PI than that provided by this section. **Other Key Provisions:** • **[Effective Jan. 1, 2016: Unlawful Practice.** Violation of the statute is an unlawful practice under ORS 646.607 (Unlawful Trade Practice).**]** • **Delay for Law Enforcement.** Notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation and that agency has made a written request that the notification be delayed. The required notification shall be made after that law enforcement agency determines that its disclosure will not compromise the investigation and notifies the Entity in writing.

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

Pennsylvania

73 Pa. Stat. § 2301 *et seq.*

S.B. 712 (signed into law Dec. 22, 2005, Act No. 94)

Effective June 20, 2006

[back to table of contents]

Application. Any state agency, political subdivision, or an individual or a business (collectively, Entity) doing business in PA that maintains, stores or manages computerized data that includes PI of PA residents.

- The provisions governing maintenance of PI that the Entity does not own appear applicable to any Entity maintaining PI, whether or not the Entity conducts business in PA.

Security Breach Definition. 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 of PI by an employee or agent of the Entity for the purposes of the Entity is not a breach of the security of the system if the PI is not used for a purpose other than the lawful purpose of the Entity and is not subject to further unauthorized disclosure.

Notification Obligation. Any Entity to which the statute applies shall provide notice of any breach of the security of the system following discovery of the breach of the security of the system to any individual whose principal mailing address, as reflected in the computerized data which is maintained, stored or managed by the Entity, is in PA whose unencrypted and unredacted PI was or is reasonably believed to have been accessed and acquired by an unauthorized person.

- An Entity must provide notice of the breach if encrypted information is accessed and acquired in an unencrypted form, if the security breach is linked to a breach of the security of the encryption or if the security breach involves a person with access to the encryption.

Notification to Consumer Reporting Agencies. When an Entity provides notification under this act to more than 1,000 persons at one time, the Entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution and number of notices.

Third-Party Data Notification. An Entity that maintains, stores or manages computerized data on behalf of another Entity shall provide notice of any breach of the security system following discovery to the Entity on whose behalf it maintains, stores or manages the data.

Timing of Notification. Except in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system, the notice shall be made without unreasonable delay.

Personal Information Definition. An individual's first name or first initial and last name in combination with and linked to any one or more of the following data elements when the data elements are not encrypted or redacted:

- Social Security Number;
- Driver license number or state identification card number issued in lieu of a driver license; or
- Account number or credit card number or debit card number in combination with any required security code, access code or password that would permit access to an individual's financial account.

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	PI does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. **Notice Required.** Notice may be provided by any of the following methods: • Written notice to the last known home address for the individual; • Telephonic notice, if the customer can be reasonably expected to receive it and the notice is given in a clear and conspicuous manner, describes the incident in general terms and verifies PI but does not require the customer to provide PI, and the customer is provided with a telephone number to call or Internet Web site to visit for further information or assistance; or • Email notice, if a prior business relationship exists and the Entity has a valid email address for the individual. **Substitute Notice Available.** If the Entity demonstrates that the cost of providing notice would exceed $100,000, the affected class of subject persons to be notified exceeds 175,000, or the Entity does not have sufficient contact information. Substitute notice shall consist of all of the following: • Email notice when the Entity has an email address for the subject persons; • Conspicuous posting of the notice on the Entity's Web site if the Entity maintains one; and • Notification to major statewide media. **Exception: Own Notification Policy.** An Entity that maintains its own notification procedures as part of an information privacy or security policy for the treatment of PI and is consistent with the notice requirements of this act shall be deemed to be in compliance with the notification requirements of this act if it notifies subject persons in accordance with its policies in the event of a breach of security. **Exception: Compliance with Other Laws.** • **Compliance with Primary Regulator.** An Entity that complies with the notification requirements or procedures pursuant to the rules, regulations, procedures or guidelines established by the Entity's primary or functional federal regulator shall be in compliance with this act. • **Federal Interagency Guidance.** 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 in compliance with this act. **Other Key Provisions:** • **Delay for Law Enforcement.** Notification required may be delayed if a law enforcement agency determines and advises the Entity in writing, specifically referencing the statute, that the notification will impede a criminal or civil investigation. The required notification shall be made after the law enforcement agency determines that it will not compromise the investigation or

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	national or homeland security. • **AG Enforcement.** The AG shall have exclusive authority to bring an action under the Unfair Trade Practices and Consumer Protection Law for a violation of the statute.

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

Puerto Rico

10 L.P.R.A. St § 4051 *et seq*.

H.B. 1184 (Signed into law Sept. 7, 2005, No. 111).

Effective January 5, 2006

[back to table of contents]

Application. Any entity that is the owner or custodian of a database that includes personal information of residents of Puerto Rico.

Violation of Security System Definition. Any situation in which it is detected that access has been permitted to unauthorized persons or entities to the data files so that the security, confidentiality or integrity of the information in the data bank has been compromised; or when normally authorized persons or entities have had access and it is known or there is reasonable suspicion that they have violated the professional confidentiality or obtained authorization under false representation with the intention of making illegal use of the information.

- This includes both access to the data banks through the system and physical access to the recording media that contain the same and any removal or undue retrieval of said recordings.

Notification Obligation. Any entity to which the statute applies must notify citizens of any breach of the security system when the breached database contains, in whole or in part, personal information files not protected by encrypted code but only by a password.

Third-Party Data Notification. Any entity that as part of their operations resells or provides access to digital data banks that at the same time contain personal information files of citizens must notify the proprietor, custodian or holder of said information of any violation of the system's security that has allowed access to those files to unauthorized persons

Timing of Notification. 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.

Personal Information Definition. At least the name or first initial and the surname of a person, together with any of the following data so that an association may established between certain information with another and in which the information is legible enough so that in order to access it there is no need to use a special cryptographic code.

- Social Security Number.
- Driver license number, voter's identification or other official identification.
- Bank or financial account numbers of any type with or without passwords or access code that may have been assigned.
- Names of users and passwords or access codes to public or private information systems.
- Medical information protected by the Health Insurance Portability and Accountability Act.
- Tax information.
- Work-related evaluations.

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

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	the citizens in general. **Notice Required.** The notice of the security system breach shall be submitted in a clear and conspicuous manner and should describe the breach in general terms and the type of sensitive information compromised. The notification shall also include a toll free number and an Internet site for people to use in order to obtain information or assistance. Notice may be provided by one of the following methods: • Written notice; or • Authenticated electronic means according to the Digital Signatures Act. **Substitute Notice Available.** When the cost of notifying all those potentially affected or of identifying them is excessively onerous due to the number of persons affected, to the difficulty in locating all persons or to the economic situation of the enterprise or entity; or whenever the cost exceeds one hundred thousand dollars ($100,000) or the number of persons exceeds one hundred thousand [(100,000)], the entity shall issue the notice through the following two (2) steps: • Prominent display of an announcement to that respect at the entities premises, on the web page of the entity, if any, and in any informative flier published and sent through mailing lists both postal and electronic; and • A communication to that respect to the media informing of the situation and providing information as to how to contact the entity to allow for better follow-up. When the information is of relevance to a specific professional or commercial sector, the announcement may be made through publications or programming of greater circulation oriented towards that sector. **Exception:** Conflict with preexisting institutional security polices. No provision of this chapter shall be interpreted as being prejudicial to those institutional information and security policies that an enterprise or entity may have in force prior to its effectiveness and whose purpose is to provide protection equal or better to the information on security herein established.

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

Rhode Island

R.I. Gen. Laws § 11- 49.2-1 *et seq*.; will be repealed effective June 26, 2016 and replaced by § 11- 49.3-1, *et seq.*

H.B. 6191 (became law without Governor's signature, July 10, 2005, Chapter 225)

Effective March 1, 2006

S.B. 0134 (enacted 6/26/15)

Effective June 26, 2016

[back to table of contents]

Application. A municipal agency, state agency, individual, sole proprietorship, partnership, association, corporation, or joint venture, business or legal entity, trust, estate, cooperative or other commercial entity (collectively, Entity) that stores, owns, collects, processes, maintains, acquires, uses or licenses data that includes PI.

Security Breach Definition. Unauthorized access or acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of PI maintained by the Entity.

- Good-faith acquisition of PI by an employee or agent of the Entity for the purposes of the Entity is not a breach of the security of the system, provided that the PI is not used or subject to further unauthorized disclosure.

Notification Obligation. Any Entity to which the statute applies shall provide notification of any disclosure of PI or any breach of the security of the system which poses a significant risk of identity theft to any resident of RI whose unencrypted PI was, or is reasonably believed to have been, acquired by an unauthorized person or entity.

Attorney General and Credit Reporting Agency Notification. In the event that more than 500 Rhode Island residents are to be notified, the Entity shall notify the attorney general and the major credit reporting agencies as to the timing, content and distribution of the notices and the approximate number of affected individuals. Notification to the attorney general and the major credit reporting agencies shall be made without delaying notice to affected Rhode Island residents.

Timing of Notification. The notification shall be made in the most expedient time possible but no later than 45 calendar days after confirmation of the breach and the ability to ascertain the information required to fulfill the notice requirements and shall be consistent with the legitimate needs of law enforcement.

Personal Information Definition. An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or are in hard copy paper format:

- Social Security Number;
- Driver license number or RI identification card number or tribal identification number; or
- Account number or credit card number or debit card number in combination with any required security code, access code, password, or personal identification number that would permit access to an individual's financial account;
- medical or health insurance information; or
- e-mail address with any required security code, access code, or password that would permit access to an individual's personal, medical, insurance or financial account.

"Encrypted" means the transformation of data through the use of a 128 bit or higher algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key. Data shall not be considered to be encrypted if it is acquired in combination with any key, security code, or password that would permit access to the encrypted data.

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. **Notice Required.** Notice may be provided by any of the following methods: • Written notice; or • Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 (E-SIGN Act). The notification to individuals must include the following information to the extent known: (1) A general and brief description of the incident, including how the security breach occurred and the number of affected individuals; (2) The type of information that was subject to the breach; (3) Date of breach, estimated date of breach or the date range within which the breach occurred; (4) Date that the breach was discovered; (5) A clear and concise description of any remediation services offered to affected individuals including toll free numbers and websites to contact: (i) The credit reporting agencies; (ii) remediation service providers; (iii) the attorney general; and (6) A clear and concise description of: the consumer's ability to file or obtain a police report; how a consumer requests a security freeze and the necessary information to be provided when requesting the security freeze; and that fees may be required to be paid to the consumer reporting agencies. **Substitute Notice Available.** If the Entity demonstrates that the cost of providing notice would exceed $25,000, or that the affected class of subject persons to be notified exceeds 50,000, or the Entity does not have sufficient contact information. Substitute notice shall consist of all of the following: • Email notice when the Entity has an email address for the subject persons; • Conspicuous posting of the notice on the Entity's Web site if the Entity maintains one; and • Notification to major statewide media. **Exception: Own Notification Policy.** Any Entity that maintains its own security breach procedures as part of an information security policy for the treatment of PI and otherwise complies with the timing requirements of the statute, shall be deemed to be in compliance with the security breach notification, provided such Entity notifies subject persons in accordance with such Entity's policies in the event of a breach of security. **Exception: Compliance with Other Laws.** • **Compliance with Primary Regulator.** Any Entity that maintains a security breach procedure pursuant to the rules, regulations, procedures or guidelines established by the primary or functional regulator shall be deemed to be in compliance with the security breach notification requirements of this section, provided such Entity notifies subject persons in accordance with the policies or the rules, regulations, procedures or guidelines established by the primary or functional regulator in the event of a breach of security

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	of the system. • **Federal Interagency Guidance.** A financial institution, trust company, credit union or its affiliates that is subject to and examined for, and found in compliance with the Federal Interagency Guidelines on Response Programs for Unauthorized Access to Customer Information and Customer Notice shall be deemed in compliance with this chapter. • **HIPAA-Covered Entities.** A provider of health care, health care service plan, health insurer, or a covered entity governed by the medical privacy and security rules issued by the federal Department of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) shall be deemed in compliance with this chapter. **Penalties.** Each reckless violation is a civil violation for which a penalty of not more than $100 per record may be adjudged against a defendant. Each knowing and willful violation of this chapter is a civil violation for which a penalty of not more than $200 per record may be adjudged against a defendant. Whenever the attorney general has reason to believe that a violation has occurred and that proceedings would be in the public interest, the attorney general may bring an action in the name of the state against the business or person in violation. **Other Key Provisions:** • **Delay for Law Enforcement.** The notification required by this section may be delayed if a federal, state or local law enforcement agency determines that the notification will impede a criminal investigation. The law enforcement agency must notify the Entity of the request to delay notification without unreasonable delay. If notice is delayed due to such determination then as soon as the law enforcement agency determines and informs the Entity that notification no longer poses a risk of impeding an investigation, notice shall be provided, as soon as practicable. The Entity shall cooperate with law enforcement in its investigation of any breach of security or unauthorized acquisition or use, which shall include the sharing of information relevant to the incident; provided however, that such disclosure shall not require the disclosure of confidential business information or trade secrets. • **Waiver Not Permitted.**

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

South Carolina

S.C. Code § 39-1-90

S.B. 453 (signed into law April 2, 2008)

Effective July 1, 2009

H.B. 3248 (signed into law April 23, 2013)

Effective April 23, 2013

[back to table of contents]

Application. A natural person, an individual, or a corporation, government or governmental subdivision or agency, trust, estate, partnership, cooperative or association (collectively, Entity) conducting business in SC, and owning or licensing computerized data or other data that includes PI.

Security Breach Definition. Unauthorized access to and acquisition of computerized data that was not rendered unusable through encryption, redaction, or other methods that compromises the security, confidentiality, or integrity of PI maintained by the Entity, 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.

- Good-faith acquisition of PI by an employee or agent of the Entity for the purposes of its business is not a breach of the security of the system if the PI is not used or subject to further unauthorized disclosure.

Notification Obligation. Any Entity to which the statute applies shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of SC whose unencrypted and unredacted PI was, or is reasonably believed to have been, acquired by an unauthorized person when the illegal use of the information has occurred or is reasonably likely to occur or use of the information creates a material risk of harm to the resident.

Notification to Consumer Reporting Agencies. If an Entity provides notice to more than 1,000 persons at one time pursuant to the statute, the Entity shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on a nationwide basis of the timing, distribution, and content of the notice.

Attorney General/Agency Notification. If an Entity provides notice to more than 1,000 SC residents, the Entity shall notify, without unreasonable delay, the Consumer Protection Division of the Department of Consumer Affairs of the timing, distribution, and content of the notice.

Third-Party Data Notification. An Entity conducting business in SC and maintaining computerized data or other data that includes PI that the Entity does not own shall notify the owner or licensee of the information of a breach of the security of the data immediately following discovery, if the PI was, or is reasonably believed to have been, acquired by an unauthorized person.

Timing of Notification. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

Personal Information Definition. The first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of SC, when the data elements are neither encrypted nor redacted:

- Social Security Number;
- Driver license number or state identification card number issued instead of a driver license;
- Financial account number or credit card number or debit card number in combination with any required security code, access code, or password that would permit access to a resident's financial account; or
- Other numbers or information that may be used to access a

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

person's financial accounts or numbers or information issued by a governmental or regulatory entity that uniquely will identify an individual.

PI does 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.

Notice Required. Notice may be provided by one of the following methods:

- Written notice;
- Telephonic notice; or
- Electronic notice, if the person's primary method of communication with the individual is by electronic means or is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 (E-SIGN Act).

Substitute Notice Available. If the Entity demonstrates that the cost of providing notice exceeds $250,000, or that the affected class of subject persons to be notified exceeds 500,000, or the person has insufficient contact information. Substitute notice consists of:

- Email notice when the Entity has an email address for the subject persons;
- Conspicuous posting of the notice on the Entity's Web site if the Entity maintains one; and
- Notification to major statewide media.

Exception: Own Notification Policy. An Entity that maintains its own notification procedures as part of an information security policy for the treatment of PI and is otherwise consistent with the timing requirements of the statute shall be deemed to be in compliance with the notification requirements of the statute if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.

Exception: Compliance with Other Laws.

- **Gramm-Leach-Bliley Act.** This section does not apply to a bank or financial institution that is subject to and in compliance with the privacy and security provisions of the Gramm-Leach-Bliley Act.
- **Interagency Guidance.** A financial institution that is subject to and in compliance with the federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice, issued March 7, 2005, by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision, as amended, is considered to be in compliance with this section.

Penalties. A person who knowingly and willfully violates this section is subject to an administrative fine of $1,000 for each resident whose information was accessible by reason of the breach, the amount to be decided by the Department of Consumer Affairs.

Other Key Provisions:

- **Delay for Law Enforcement.** The notification required by the

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	statute may be delayed if a law enforcement agency determines that the notification impedes a criminal investigation. The notification required by the statute must be made after the law enforcement agency determines that it no longer compromises the investigation. • **Private Right of Action.** A resident of SC 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 in case of a willful and knowing violation; institute a civil action to recover only actual damages resulting from a violation in case of a negligent violation; seek an injunction to enforce compliance; and recover attorney's fees and court costs, if successful.

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

Tennessee

Tenn. Code § 47-18-2107

H.B. 2170 (signed into law June 8, 2005, Chapter 473)

Effective July 1, 2005

S.B. 2005 (signed into law March 24, 2016)

Effective July 1, 2016

[back to table of contents]

Application. Any person or business that conducts business in TN, or any agency of TN or any of its political subdivisions (collectively, Entity), that owns or licenses computerized data that includes PI.

- The provisions governing maintenance of PI that the Entity does not own appear applicable to any Entity maintaining PI, whether or not the Entity conducts business in TN.

Security Breach Definition. Unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of PI maintained by the Entity.

- Good-faith acquisition of PI by an employee or agent of the Entity for the purposes of the Entity is not a breach of the security of the system, provided that the PI is not used or subject to further unauthorized disclosure.

Notification Obligation. Any Entity to which the statute applies shall disclose any breach of the security of the system, following discovery or notification of the breach in the security of the data, to any resident of TN whose PI was, or is reasonably believed to have been, acquired by an unauthorized person. "Unauthorized person" includes an employee of the information holder who is discovered by the information holder to have obtained personal information and intentionally used it for an unlawful purpose. **Note:** effective July 1, 2016, the word "unencrypted" was deleted from the definition of "breach" and the notification obligation, but the definition of "personal information" was not changed.

Notification to Consumer Reporting Agencies. If an Entity is required to notify more than 1,000 persons at one time, the person shall also notify, without unreasonable delay, all consumer reporting agencies and credit bureaus that compile and maintain files on consumers on a nationwide basis of the timing, distribution and content of the notices.

Third-Party Data Notification. Any Entity that maintains computerized data that includes PI that the Entity does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately, but no later than 45 days from when the breach became known by the information holder, if the PI was, or is reasonably believed to have been, acquired by an unauthorized person.

Timing of Notification. The disclosure shall be made immediately, but no later than 45 days from the discovery or notification of the breach, unless a longer period of time is required due to the legitimate needs of law enforcement.

Personal Information Definition. An individual's first name or first initial and last name, in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

- Social Security Number;
- Driver license number; or
- Account number or credit card number or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.

PI does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	Notice Required. Notice may be provided by one of the following methods: • Written notice; or • Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 (E-SIGN Act). **Substitute Notice Available.** If the Entity demonstrates that the cost of providing notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000, or the Entity does not have sufficient contact information. Substitute notice shall consist of all of the following: • Email notice when the Entity has an email address for the subject persons; • Conspicuous posting of the notice on the Entity's Web site if the Entity maintains one; and • Notification to major statewide media. **Exception: Own Notification Policy.** An Entity that maintains its own notification procedures as part of an information security policy for the treatment of PI and is otherwise consistent with the timing requirements of the statute shall be deemed to be in compliance with the notification requirements of the statute if it notifies subject persons in accordance with its policies in the event of a breach of security of the system. **Exception: Compliance with Other Laws.** The provisions of this statute shall not apply to any Entity that is subject to: • The provisions of Title V of the Gramm-Leach-Bliley Act. • The Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1320d), as expanded by the Health Information Technology for Clinical and Economic Health Act **Other Key Provisions:** • **Delay for Law Enforcement.** The notification required may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made no later than 45 days after the law enforcement agency determines that it will not compromise the investigation. • **Private Right of Action.**

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

Texas

Tex. Bus. & Com. Code §§ 521.002, 521.053

Acts 2007, 80th Leg., ch. 885, § 2.01. Amended by Acts 2009, 81st Leg., ch. 419, § 3.

Effective April 1, 2009

Acts 2011, 82nd Leg., ch. 1126, § 14 (H.B. No. 300).

Effective Sept. 1, 2012

S.B. 1610 (signed into law June 14, 2013)

Effective June 14, 2013

[back to table of contents]

Application. A person (Entity) that conducts business in TX and owns or licenses computerized data that includes sensitive PI.

- The provisions governing maintenance of sensitive PI that the Entity does not own appear applicable to any Entity maintaining PI, whether or not the Entity conducts business in TX.

Security Breach Definition. Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive PI maintained by an Entity, including data that is encrypted if the person accessing the data has the key required to decrypt the data.

- Good-faith acquisition of sensitive PI by an employee or agent of the Entity for the purposes of the Entity is not a breach of system security unless the sensitive PI is used or disclosed by the person in an unauthorized manner.

Notification Obligation. Any Entity to which the statute applies shall disclose any breach of system security, after discovering or receiving notification of the breach, to any person, including nonresidents, whose sensitive PI was, or is reasonably believed to have been, acquired by an unauthorized person.

Notification to Consumer Reporting Agencies. If an Entity is required by this section to notify at one time more than 10,000 persons of a breach of system security, the Entity shall also notify, without unreasonable delay, all consumer reporting agencies that maintain files on consumers on a nationwide basis of the timing, distribution, and content of the notices.

Third-Party Data Notification. Any Entity that maintains computerized data that includes sensitive PI that the Entity does not own shall notify the owner or license holder of the information of any breach of system security immediately after discovering the breach, if the sensitive PI was, or is reasonably believed to have been, acquired by an unauthorized person.

Timing of Notification. The disclosure shall be made as quickly as possible, consistent with the legitimate needs of law enforcement or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

Sensitive Personal Information Definition. An individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted:

- Social Security Number;
- Driver license number or government-issued ID number; or
- Account number or credit card number or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Sensitive PI also includes information that identifies an individual and relates to:

- The physical or mental health or condition of the individual;
- The provision of health care to the individual; or
- Payment for the provision of health care to the individual.

Sensitive PI does not include publicly available information that is lawfully made available to the general public from the federal government or a state or local government.

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	Notice Required. Notice may be provided by one of the following methods: • Written notice at the last known address of the individual; or • Electronic notice, if the notice is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 (E-SIGN Act). However, if the affected person is a resident of a state that has its own breach notification requirement, the Entity may provide notice under that state's law or under Texas's law. **Substitute Notice Available.** If the Entity demonstrates that the cost of providing notice would exceed $250,000, the number of affected persons exceeds 500,000, or the Entity does not have sufficient contact information, the notice may be given by any of the following: • Email notice when the Entity has an email address for the affected persons; • Conspicuous posting of the notice on the Entity's Web site; or • Notice published in or broadcast on major statewide media. **Exception: Own Notification Policy.** An Entity that maintains its own notification procedures as part of an information security policy for the treatment of sensitive PI that complies with the timing requirements for notice under this section complies with this section if the Entity notifies affected persons in accordance with that policy. **Other Key Provisions:** • **Delay for Law Enforcement.** An Entity may delay providing notice as required at the request of a law enforcement agency that determines that the notification will impede a criminal investigation. The required notification shall be made as soon as the law enforcement agency determines that the required notice will not compromise the investigation. • **AG Enforcement.** Remedies include injunctive relief and civil penalties of at least $2,000 but not more than $50,000 for each violation. • Civil penalties for failure to comply with notification requirements are raised to up to $100 per person to whom notification is due, per day, not to exceed $250,000 per breach.

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

Utah

Utah Code §§ 13-44-101, 13-44-202, 13-44-301

S.B. 69 (signed into law March 20, 2006, Session Law Chapter 343)

Effective January 1, 2007

S.B. 208 (signed into law March 30, 2009)

Effective May 12, 2009

[back to table of contents]

Application. Any Entity who owns or licenses computerized data that includes PI concerning a UT resident.

Security Breach Definition. Unauthorized acquisition of computerized data maintained by an Entity that compromises the security, confidentiality, or integrity of PI.

- Does not include the acquisition of PI by an employee or agent of the Entity possessing unencrypted computerized data unless the PI is used for an unlawful purpose or disclosed in an unauthorized manner.

Notification Obligation. If investigation reveals that the misuse of PI for identity theft or fraud has occurred, or is reasonably likely to occur, the person shall provide notification to each affected UT resident.

- Notification is not required if after a good-faith, reasonable and prompt investigation the Entity determines that it is unlikely that PI has been or will be misused for identity theft or fraud.

Third-Party Data Notification. An Entity that maintains computerized data that includes PI that the Entity does not own or license shall notify and cooperate with the owner or licensee of the information of any breach of system security immediately following the Entity's discovery of the breach if misuse of the PI occurs or is reasonably likely to occur.

Timing of Notification. Notification shall be provided in the most expedient time possible without unreasonable delay, after determining the scope of the breach of system security and after restoring the reasonable integrity of the system.

Personal Information Definition. A person's first name or first initial and last name, combined with any one or more of the following data elements relating to that person when either the name or data element is unencrypted or not protected by another method that renders the data unreadable or unusable:

- Social Security Number;
- Driver license number or state identification card number; or
- Account number or 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 account.

PI does not include information regardless of its source, contained in federal, state, or local government records or in widely distributed media that are lawfully made available to the general public.

Notice Required. Notice may be provided by one of the following methods:

- In writing by first-class mail to the most recent address the Entity has for the resident;
- By telephone, including through the use of automatic dialing technology not prohibited by other law;
- Electronically, if the Entity's primary method of communication with the resident is by electronic means, or if provided consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 (E-SIGN Act); or
- By publishing notice of the breach of system security in a newspaper of general circulation. Such notice must comply with Utah Code § 45-1-101.

Substitute Notice. Substitute notice is not available in UT.

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	Exception: Own Notification Policy. If an Entity maintains its own notification procedures as part of an information security policy for the treatment of PI the Entity is considered to be in compliance with this chapter's notification requirements if the procedures are otherwise consistent with this chapter's timing requirements and the Entity notifies each affected UT resident in accordance with the Entity's information security policy in the event of a breach. **Exception: Compliance with Other Laws.** An Entity who is regulated by state or federal law and maintains procedures for a breach of system security under applicable law established by the primary state or federal regulator is considered to be in compliance with this part if the Entity notifies each affected UT resident in accordance with the other applicable law in the event of a breach. **Penalties.** Violators are subject to a civil fine of no more than $2,500 for a violation or series of violations concerning a specific consumer and no more than $100,000 in the aggregate for related violations concerning more than one consumer. **Other Key Provisions:** • **Delay for Law Enforcement.** An Entity may delay providing notification at the request of a law enforcement agency that determines that notification may impede a criminal investigation. Notification shall be provided in good faith, without unreasonable delay, and in the most expedient time possible after the law enforcement agency informs the person that notification will no longer impede the criminal investigation. • **AG Enforcement.** • **Waiver Not Permitted.**

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

Vermont

9 V.S.A. §§ 2430, 2435

S. 284 (signed into law May 18, 2006, Act 162). Amended by H. 254 (signed into law May 8, 2012, Act 109).

Effective May 8, 2012.

H. 513 (signed into law May 13, 2013)

Effective May 13, 2013

S. 73 (signed into law June 9, 2015)

Effective July 1, 2015

[back to table of contents]

Application. Any data collector, including, but not limited to, the state, state agencies, political subdivisions of the state, public and private universities, privately and publicly held corporations, limited liability companies, financial institutions, retail operators, and any other entity that, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates, or otherwise deals with nonpublic PI (Entity), that owns or licenses computerized PI that includes PI concerning an individual residing in VT.

Security Breach Definition. Unauthorized acquisition of electronic data or a reasonable belief of such unauthorized acquisition that compromises the security, confidentiality, or integrity of PI maintained by an Entity.

- Does not include good-faith but unauthorized acquisition or access of PI by an employee or agent of the Entity for a legitimate purpose of the Entity, provided that the PI is not used for a purpose unrelated to the Entity's business or subject to further unauthorized disclosure.

To determine whether this definition applies, any Entity may consider the following factors (among others):

- Indications that the information is in the physical possession and control of a person without valid authorization, such as a lost or stolen computer or other device containing information;
- Indications that the information has been downloaded or copied;
- Indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported; or
- That the information has been made public.

Notification Obligation. An Entity shall notify affected individuals residing in VT that there has been a security breach following discovery or notification to the Entity of the breach.

- Notice of a security breach is not required if the Entity establishes that misuse of PI is not reasonably possible and the Entity provides notice of the determination that the misuse of the PI is not reasonably possible and a detailed explanation for said determination to the VT AG or to the Department of Banking, Insurance, Securities, and Health Care Administration in the event that the Entity is a person or entity licensed or registered with the Department.

Notification to Consumer Reporting Agencies. In the event an Entity is required to provide notice to more than 1,000 residents of VT at one time, the Entity shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution, and content of the notice. This subsection shall not apply to a person who is licensed or registered under Title 8 by the department of banking, insurance, securities, and health care administration.

Attorney General/Agency Notification. An Entity shall notify the AG or Department of Financial Regulation of any breach within 14 business days of the date the Entity discovers the breach or the date the Entity provides notice to consumers, whichever is sooner.

Any Entity that has, prior to the breach, sworn in writing on a form and in a manner prescribed by the AG that the Entity maintains written policies and procedures to maintain the security of PI and respond to breaches in a

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	manner consistent with state law shall notify the AG before providing notice to consumers. Notice to the AG shall contain the date the breach occurred, the date the breach was discovered, and a description of the breach. If the date of the breach is unknown, then the Entity shall send notice to the AG or the Department as soon as the date becomes known. If an Entity provides notice of the breach to consumers, the Entity shall notify the AG or the Department of the number of Vermont affected, if known, and shall provide a copy of the notice that was provided to consumers. An Entity may also send the AG or Department a second copy of the notice to consumers that redacts the type of PI breached for any public disclosure of the breach. **Third-Party Data Notification.** Any Entity that maintains or possesses computerized data containing PI of an individual residing in VT that the Entity does not own or license or any Entity that conducts business in VT that maintains or possesses records or data containing PI that the Entity does not own or license shall notify the owner or licensee of the information of any security breach immediately following discovery of the breach, consistent with the legitimate needs of law enforcement. **Timing of Notification.** Notice of the breach shall be made in the most expedient time possible and without unreasonable delay, but not later than 45 days after the discovery of the breach, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system. **Personal Information Definition.** An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted or protected by another method that renders them unreadable or unusable by unauthorized persons: • Social Security Number; • Motor vehicle operator's license number or nondriver identification card number; • Account number or credit card number or debit card number if circumstances exist in which the number could be used without additional identifying information, access codes, or passwords; or • Account passwords or personal identification numbers or other access codes for a financial account. PI does not mean publicly available information that is lawfully made available to the general public from federal, state, or local government records. **Notice Required.** The notice to a consumer shall be clear and conspicuous and include a description of each of the following, if known to the Entity: • The incident in general terms; • The type of PI that was subject to the security breach; • The general acts of the Entity to protect the PI from further security breach; • A telephone number (toll-free, if available) that the consumer may call for further information and assistance; • Advice that directs the consumer to remain vigilant by reviewing account statements and monitoring free credit reports; and • The approximate date of the security breach.

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	Notice may be provided by one or more of the following methods: • Written notice mailed to the individual's residence; • Telephonic notice, provided that telephonic contact is made directly with each affected resident of VT, and not through a prerecorded message; or • Electronic notice, for those individuals for whom the Entity has a valid e-mail address if (i) the Entity's primary method of communication with the individual is by electronic means, the electronic notice does not request or contain a hypertext link to a request that the individual provide PI, and the electronic notice conspicuously warns individuals not to provide PI in response to electronic communications regarding security breaches; or (ii) the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 (E-SIGN Act). **Substitute Notice Available.** If the Entity demonstrates that the cost of providing written or telephonic notice to affected residents would exceed $5,000, or that the affected class of affected residents to be provided written or telephonic notice exceeds 5,000, or the Entity does not have sufficient contact information. Substitute notice shall consist of all of the following: • Conspicuously posting the notice on the Entity's Web site if the Entity maintains one; and • Notifiying major statewide and regional media. **Exception: Compliance with Other Laws.** • A financial institution that is subject to the following guidance, and any revisions, additions, or substitutions relating to said interagency guidance shall be exempt from this section: (i) The Federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice, issued on March 7, 2005, by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision; or (ii) Final Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice, issued on April 14, 2005, by the National Credit Union Administration. **Other Key Provisions:** • **Delay for Law Enforcement.** The required notice to a consumer shall be delayed upon request of a law enforcement agency. A law enforcement agency may request the delay if it believes that notification may impede a law enforcement investigation, or a national or homeland security investigation, or jeopardize public safety or national or homeland security interests. In the event law enforcement makes the request in a manner other than in writing, the Entity shall document such request contemporaneously in writing, including the name of the law enforcement officer making the request and the officer's law enforcement agency engaged in

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	the investigation. The Entity shall provide the required notice without unreasonable delay upon receipt of a written communication, which includes facsimile or electronic communication, from the law enforcement agency withdrawing its request for delay. • **AG Enforcement.** • **Waiver Not Permitted.**

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

Virginia

Va. Code § 18.2-186.6 (effective July 1, 2008), § 32.1-127.1:05 (effective January 1, 2011)

[back to table of contents]

Application. An individual, corporation, business trust, estate, partnership, limited partnership, limited liability partnership, limited liability company, association, organization, joint venture, government, governmental subdivision, agency, or instrumentality or any other legal entity, whether for profit or not for profit (collectively, Entity) that owns or licenses computerized data that includes PI.

- A separate provision covering health information applies only to government entities, defined as any authority, board, bureau, commission, district or agency of the Commonwealth or of any political subdivision of the Commonwealth, including cities, towns and counties, municipal councils, governing bodies of counties, school boards and planning commissions; boards of visitors of public institutions of higher education; and other organizations, corporations, or agencies in VA supported wholly or principally by public funds.

Security Breach Definition. Unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of PI maintained by an Entity as part of a database of PI regarding multiple individuals and that causes, or the Entity reasonably believes has caused, or will cause, identity theft or other fraud to any resident of VA.

- Good-faith acquisition of PI by an employee or agent of an Entity for the purposes of the Entity is not a breach of the security of the system, provided that the PI is not used for a purpose other than a lawful purpose of the individual or entity or subject to further unauthorized disclosure.

Notification Obligation. If unencrypted or unredacted PI was or is reasonably believed to have been accessed and acquired by an unauthorized person and causes, or the Entity reasonably believes has caused or will cause, identity theft or another fraud to any resident of VA, an Entity to which the statute applies shall disclose any breach of the security of the system following discovery or notification of the breach of the security of the system to any affected resident of VA.

- An Entity shall disclose the breach of the security of the system 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 Entity reasonably believes that such a breach has caused or will cause identity theft or other fraud to any resident of VA.
- For health information, the Entity must notify both the subject of the medical information and any affected resident of the VA, if those are not the same person.

Notification to Consumer Reporting Agencies. In the event an Entity provides notice to more than 1,000 persons at one time pursuant to the general security breach section, the Entity shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. Section 1682(a)(p), of the timing, distribution, and content of the notice.

Attorney General/Agency Notification. The state AG must be notified whenever any VA residents are notified under the criteria above. In the event an 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,

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	the state AG of the timing, distribution, and content of the notice. For health information, the Entity must also notify the Commissioner of Health. **Third-Party Data Notification.** An Entity that maintains computerized data that includes PI that the Entity does not own or license shall notify the owner or licensee of the information of any breach of the security of the system without unreasonable delay following discovery of the breach of the security of the system, if the PI was accessed and acquired by an unauthorized person or the Entity reasonably believes the PI was accessed and acquired by an unauthorized person. **Timing of Notification.** Notice required by the statute shall be made without unreasonable delay. Notice may be reasonably delayed to allow individual or entity to determine scope of the breach of security and restore the reasonable integrity of the system. **Personal Information Definition.** The first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of VA, when the data elements are neither encrypted nor redacted: • Social Security Number; • Driver license number or state identification card number issued in lieu of a driver license number; or • Account number or credit card number or debit card number in combination with any required security code, access code, or password that would permit access to a resident's financial accounts. The health information breach law applies to the first name or first initial and last name with any of the following elements: • Any information regarding an individual's medical or mental health history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or • An individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records. PI does 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. **Notice Required.** Notice shall include a description of the following: • The incident in general terms; • The type of PI or medical information that was subject to the unauthorized access and acquisition; • The general acts of the individual or entity to protect the PI from further unauthorized access; • A telephone number that the person may call for further information and assistance, if one exists; and • Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports. Notice means: • Written notice to the last known postal address in the records of

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	the individual or entity; • Telephone notice; or • Electronic notice. **Substitute Notice Available.** If the Entity demonstrates that the cost of providing notice will exceed $50,000, the affected class of VA residents to be notified exceeds 100,000 residents, or the individual or the entity does not have sufficient contact information or consent to provide written, electronic or telephonic notice. Substitute notice consists of all of the following: • E-mail notice if the individual or the entity has e-mail addresses for the members of the affected class of residents; • Conspicuous posting of the notice on the Entity's Web site if the Entity maintains one; and • Notice to major statewide media. **Exception: Own Notification Policy.** An Entity that maintains its own notification procedures as part of an information privacy or security policy for the treatment of PI that are consistent with the timing requirements of this section shall be deemed to be in compliance with the notification requirements of this section if it notifies residents of VA in accordance with its procedures in the event of a breach of the security of the system. **Exception: Compliance with Other Laws.** • **Gramm-Leach-Bliley Act.** An entity that is subject to Title V of the Gramm-Leach-Bliley Act and maintains procedures for notification of a breach of the security of the system in accordance with the provision of that Act and any rules, regulations, or guidelines promulgated thereto shall be deemed to be in compliance with this section. • **Primary Regulator.** An entity that complies with the notification requirements or procedures pursuant to the rules, regulations, procedures, or guidelines established by the entity's primary or functional state or federal regulator shall be in compliance with this section. • **HIPAA-Covered Entities.** The notification requirements for incidents involving medical information do not apply to (i) a "covered entity" or "business associate" subject to requirements for notification in the case of a breach of protected health information (42 U.S.C. § 17932 *et seq*.) or (ii) a person or entity who is a non-HIPAA-covered entity subject to the Health Breach Notification Rule promulgated by the Federal Trade Commission pursuant to 42 U.S.C. § 17937 *et seq*. **Penalties.** The state AG 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. (This provision does not apply to health information breaches.) **Other Key Provisions:** • **Delay for Law Enforcement.** Notice required by this section may be delayed if, after the Entity notifies a law enforcement

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	agency, the law enforcement agency determines and advises the Entity that the notice will impede a criminal or civil investigation, or homeland or national security. Notice shall be made without unreasonable delay after the law enforcement agency determines that the notification will no longer impede the investigation or jeopardize national or homeland security. • **AG Enforcement.**

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

Washington

Wash. Rev. Code § 19.255.010 *et seq*.

S.B. 6043 (signed into law May 10, 2005, Chapter 368)

Effective July 24, 2005

H.B. 1149 (signed into law March 22, 2010) requiring reimbursement from payment processors, businesses, and vendors to financial institutions for the cost of replacing credit and debit cards after a breach

Effective July 1, 2010

H.B. 1078 (signed into law April 23, 2015)

Effective July 24, 2015

[back to table of contents]

Application. Any state or local agency or any person or business which conducts business in WA (collectively, Entity) that owns or licenses computerized data that includes PI.

Security Breach Definition. Unauthorized acquisition of data that compromises the security, confidentiality, or integrity of PI maintained by the Entity.

- Good-faith acquisition of PI by an employee or agent of the Entity for the purposes of the Entity is not a breach of the security of the system when the PI is not used or subject to further unauthorized disclosure.

Notification Obligation. Any Entity to which the statute applies shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of WA whose PI was, or is reasonably believed to have been, acquired by an unauthorized person and [effective July 24, 2015] the personal information was not "secured" (i.e., encrypted in a manner that meets or exceeds the national institute of standards and technology (NIST) standard or is otherwise modified so that the personal information is rendered unreadable, unusable, or undecipherable by an unauthorized person) .

- [Effective July 24, 2015] Notice is not required if the breach of the security of the system is not reasonably likely to subject consumers to a risk of harm. The breach of secured personal information must be disclosed if the information acquired and accessed is not secured during a security breach or if the confidential process, encryption key, or other means to decipher the secured information was acquired by an unauthorized person.

Attorney General Notification. [Effective July 24, 2015] Any Entity that is required to issue a notification to more than 500 Washington residents as a result of a single breach shall, by the time notice is provided to affected consumers, electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the attorney general. The Entity shall also provide to the attorney general the number of Washington consumers affected by the breach, or an estimate if the exact number is not known.

Third-Party Data Notification. Any Entity that maintains computerized data that includes PI that the Entity does not own shall notify the owner or licensee of the information of any breach immediately following discovery, if the PI was, or is reasonably believed to have been, acquired by an unauthorized person.

Timing of Notification. [effective July 24, 2015] The disclosure to affected consumers and to the attorney general shall be made in the most expedient time possible and without unreasonable delay, no more than 45 calendar days after the breach was discovered, unless at the request of law enforcement or due to any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system..

Personal Information Definition. An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

- Social Security Number;
- Driver license number or Washington identification card number;
- Account number or credit card number or debit card number in

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	combination with any required security code, access code, or password that would permit access to an individual's financial account. PI does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. **Notice Required.** Notice may be provided by the following methods: • Written notice; or • Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 (E-SIGN Act). **[Effective July 24, 2015]** The notification must be written in plain language and must include, at a minimum, the following information: • The name and contact information of the reporting person or business subject to this section; • A list of the types of personal information that were or are reasonably believed to have been the subject of a breach; and • The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed personal information. **Substitute Notice Available.** If the Entity demonstrates that the cost of providing notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000, or the Entity does not have sufficient contact information. Substitute notice shall consist of <u>all</u> of the following: • Email notice when the Entity has an email address for the subject persons; • Conspicuous posting of the notice on the Entity's Web site if the Entity maintains one; and • Notification to major statewide media. **Exception: Compliance with Other Laws.** • **Certain Financial Institutions.** [Effective July 24, 2015] A financial institution under the authority of the office of the comptroller of the currency, the federal deposit insurance corporation, the national credit union administration, or the federal reserve system is deemed to have complied with respect to "sensitive customer information" as defined in the interagency guidelines establishing information security standards, 12 C.F.R. Part 30, Appendix B, 12 C.F.R. Part 208, Appendix D-2, 12 C.F.R. Part 225, Appendix F, and 12 C.F.R. Part 364, Appendix B, and 12 C.F.R. Part 748, Appendices A and B, if the financial institution provides notice to affected consumers pursuant to the interagency guidelines and the notice complies with the customer notice provisions of the interagency guidelines establishing information security standards and the interagency guidance on response programs for unauthorized access to customer information and customer notice under 12 C.F.R. Part 364 as it existed on the effective date of this section. The entity shall comply with the attorney general notification requirements here in

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

addition to providing notice to its primary federal regulator.

- **HIPAA-Covered Entities**. [Effective July 24, 2015] A covered entity under HIPAA is deemed to have complied with respect to protected health information if it has complied with section 13402 of the federal health information technology for economic and clinical health act, Public Law 111-5. Covered entities must notify the attorney general in compliance with the timeliness of notification requirements of section 13402 of the federal health information technology for economic and clinical health act, Public Law 111-5, notwithstanding the timing of notification requirements here.

Exception: Own Notification Policy. An Entity that maintains its own notification procedures as part of an information security policy for the treatment of PI and is otherwise consistent with the timing requirements of this section is in compliance with the notification requirements of this section if the Entity notifies subject persons in accordance with its policies in the event of a breach of security.

Other Key Provisions:

- **Delay for Law Enforcement.** Notification may be delayed if the data owner or licensee contacts a law enforcement agency after discovery of a breach of the security of the system and a law enforcement agency determines that the notification will impede a criminal investigation. The required notification shall be made after the law enforcement agency determines that it will not compromise the investigation.
- **AG Enforcement.** [Effective July 24, 2015] AG may bring action on behalf of state or residents. Violation is unfair or deceptive act and unfair method of competition.
- **Private Right of Action.** Any consumer injured by a violation of this section may institute a civil action to recover damages.
- **Waiver Not Permitted.**

Reimbursement from Businesses to Financial Institutions. In the event of a breach where an entity held unencrypted account information or was not PCI DSS compliant, payment processors, businesses, and vendors can be liable to a financial institution for the cost of reissuing credit and debit cards in the event of a breach that results in the disclosure of the full, unencrypted account information contained on an identification device, or the full, unencrypted account number on a credit or debit card or identification device plus the cardholder's name, expiration date, or service code.

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

West Virginia

W. VA. Code § 46A-2A-101 *et seq*.

S.B. 340 (signed into law March 27, 2008)

Effective June 6, 2008

[back to table of contents]

Application. An individual, corporation, business trust, estate, partnership, limited partnership, limited liability partnership, limited liability company, association, organization, joint venture, government, governmental subdivision, agency or instrumentality, or any other legal entity, whether for profit or not for profit, (collectively, Entity) that owns or licenses computerized data that includes PI.

Security Breach Definition. Unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of PI maintained by an Entity as part of a database of PI regarding multiple individuals and that causes the Entity to reasonably believe that the breach of security has caused or will cause identity theft or other fraud to any resident of WV.

- Good-faith acquisition of PI by an employee or agent of an Entity for the purposes of the Entity is not a breach of the security of the system, provided that the PI is not used for a purpose other than a lawful purpose of the Entity or subject to further unauthorized disclosure.

Notification Obligation. Any Entity to which the statute applies shall give notice of any breach of the security of the system following discovery or notification of the breach of the security of the system to any resident of WV whose unencrypted and unredacted PI was or is reasonably believed to have been accessed and acquired by an unauthorized person and that causes, or the individual or entity reasonably believes has caused or will cause, identity theft or other fraud to any resident of WV.

- An Entity must give notice of the breach of the security of the system 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 Entity reasonably believes that such breach has caused or will cause identity theft or other fraud to any resident of this state.

Notification to Consumer Reporting Agencies. If an Entity is required to notify more than 1,000 persons of a breach of security pursuant to this article, the Entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on a nationwide basis of the timing, distribution and content of the notices. Nothing in this subsection shall be construed to require the entity to provide to the consumer reporting agency the names or other PI of breach notice recipients.

Third-Party Data Notification. An Entity that maintains computerized data that includes PI that the Entity does not own or license shall give notice to the owner or licensee of the information of any breach of the security of the system as soon as practicable following discovery, if the PI was or the Entity reasonably believes was accessed and acquired by an unauthorized person.

Timing of Notification. Except in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the system, the notice shall be made without unreasonable delay.

Personal Information Definition. The first name or first initial and last name linked to any one or more of the following data elements that relate to a resident of WV, when the data elements are neither encrypted nor redacted:

- Social Security Number;
- Driver license number or state identification card number issued in lieu of a driver license; or

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	• Account number or credit card number or debit card number in combination with any required security code, access code or password that would permit access to a resident's financial accounts. PI does 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. **Notice Required.** The notice shall include: • To the extent possible, a description of the categories of information that were reasonably believed to have been accessed or acquired by an unauthorized person, including Social Security Numbers, driver licenses or state identification numbers and financial data; • A telephone number or Web site 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; and whether or not 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. Notice may be provided by one of the following methods: • Written notice to the postal address in the records of the Entity; • Telephonic notice; or • Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 (E-SIGN Act). **Substitute Notice Available.** If an Entity demonstrates that the cost of providing notice will exceed $50,000, or that the affected class of residents to be notified exceeds 100,000 persons, or that the Entity does not have sufficient contact information to provide notice. Substitute notice consists of any two of the following: • E-mail notice if the Entity has e-mail addresses for the members of the affected class of residents; • Conspicuous posting of the notice on the Entity's Web site if the Entity maintains one; or • Notice to major statewide media. **Exception: Own Notification Policy.** An Entity that maintains its own notification procedures as part of an information privacy or security policy for the treatment of PI and that are consistent with the timing requirements of this article shall be deemed to be in compliance with the notification requirements of this article if it notifies residents of WV in accordance with its procedures in the event of a breach of security of the system. **Exception: Compliance with Other Laws.** • **Federal Interagency Guidance.** A financial institution that responds in accordance with the notification guidelines prescribed

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	by the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice is deemed to be in compliance with this article. • **Primary Regulator.** An Entity that complies with the notification requirements or procedures pursuant to the rules, regulation, procedures or guidelines established by the Entity's primary or functional regulator shall be in compliance with this article. **Other Key Provisions:** • **Delay for Law Enforcement.** Notice required by this section may be delayed if a law-enforcement agency determines and advises the Entity that the notice will impede a criminal or civil investigation or homeland or national security. Notice required by this section must be made without unreasonable delay after the law-enforcement agency determines that notification will no longer impede the investigation or jeopardize national or homeland security. • **AG Enforcement.** • This subsection shall not apply to an entity subject to Title V of the Gramm-Leach-Bliley Act.

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

Wisconsin

Wis. Stat. § 134.98

S.B. 164 (signed into law March 16, 2006, Act 138)

Effective March 31, 2006

[back to table of contents]

Application. Any Entity that maintains or licenses PI in WI or that knows that PI pertaining to a resident of WI has been acquired by a person whom the Entity has not authorized to acquire the PI. Entity includes: the state of WI and any office, department, independent agency, authority, institution, association, society, or other body in state government created or authorized to be created by the constitution or any law, including the legislature and the courts; a city, village, town, or county; a person, other than an individual, that does any of the following:

- Conducts business in WI and maintains PI in the ordinary course of business;
- Licenses PI in WI;
- Maintains for a resident of WI a depository account;
- Lends money to a resident of WI.

Security Breach Definition. When an Entity whose principal place of business is located in WI or an Entity that maintains or licenses PI in WI knows that PI in the Entity's possession has been acquired by a person whom the Entity has not authorized to acquire the PI, or, in the case of an Entity whose principal place of business is not located in WI, when it knows that PI pertaining to a resident of WI has been acquired by a person whom the Entity has not authorized to acquire the PI.

Notification Obligation. Any Entity to which the statute applies shall make reasonable efforts to notify each subject of the PI.

- An Entity is not required to provide notice of the acquisition of PI if the acquisition of PI does not create a material risk of identity theft or fraud to the subject of the PI or if the PI was acquired in good faith by an employee or agent of the Entity, if the PI is used for a lawful purpose of the Entity.

Notification to Consumer Reporting Agencies. If, as the result of a single incident, an Entity is required to notify 1,000 or more individuals that PI pertaining to the individuals has been acquired, the Entity shall without unreasonable delay notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, of the timing, distribution, and content of the notices sent to the individuals.

Third-Party Data Notification. If a person, other than an individual, that stores PI pertaining to a resident of WI, but does not own or license the PI, knows that the PI has been acquired by a person whom the person storing the PI has not authorized to acquire the PI, and the person storing the PI has not entered into a contract with the person that owns or licenses the PI, the person storing the PI shall notify the person that owns or licenses the PI of the acquisition as soon as practicable.

Timing of Notification. An Entity shall provide the notice within a reasonable time, not to exceed 45 days after the Entity learns of the acquisition of PI. A determination as to reasonableness shall include consideration of the number of notices that an Entity must provide and the methods of communication available to the Entity.

Personal Information Definition. An individual's last name and the individual's first name or first initial, in combination with and linked to any of the following elements, if the element is not publicly available information and is not encrypted, redacted, or altered in a manner that renders the element unreadable:

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	• Social Security Number; • Driver license number or state identification number; • Account number or credit card number or debit card number or any security code, access code, or password that would permit access to the individual's financial account; • DNA profile; or • Unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation. An element is publicly available if the Entity reasonably believes that it was lawfully made widely available through any media or lawfully made available to the general public from federal, state, or local government records or disclosures to the general public that are required to be made by federal, state, or local law. **Notice Required.** The notice shall indicate that the Entity knows of the unauthorized acquisition of PI pertaining to the resident of WI who is the subject of the PI. Notice may be provided by one of the following methods: • Mail; or • A method the Entity has previously employed to communicate with the subject of the PI. **Substitute Notice Available.** If an Entity cannot with reasonable diligence determine the mailing address of the subject of the PI, and if the Entity has not previously communicated with the subject of the PI, the Entity shall provide notice by a method reasonably calculated to provide actual notice to the subject of the PI. **Exception: Compliance with Other Laws.** • **Gramm-Leach-Bliley Act.** An Entity that is subject to, and in compliance with, the privacy and security requirements of Title V of the Gramm-Leach-Bliley Act, or a person that has a contractual obligation to such an Entity, if the Entity or person has in effect a policy concerning breaches of information security. • **HIPAA-Covered Entities.** A health plan, health care clearinghouse, or health care provider who transmits any health information in electronic form, if the Entity complies with the requirements of 45 C.F.R. pt. 164. **Other Key Provisions:** • **Delay for Law Enforcement.** A law enforcement agency may, in order to protect an investigation or homeland security, ask an Entity not to provide a required notice for any period of time. If an Entity receives such a request, the Entity may not provide notice of or publicize an unauthorized acquisition of PI, except as authorized by the law enforcement agency that made the request.

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

Wyoming

Wyo. Stat. § 40-12-501 *et seq*.

Effective July 1, 2007

Senate File Nos. 35 and 36 (signed into law March 2, 2015)

Effective July 1, 2015

[back to table of contents]

Application. An individual or commercial entity (collectively, Entity) that conducts business in WY and that owns or licenses computerized data that includes PI about a resident of WY.

Security Breach Definition. Unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of PI maintained by an Entity and causes or is reasonably believed to cause loss or injury to a resident of WY.

- Good-faith acquisition of PI by an employee or agent of an Entity for the purposes of the Entity is not a breach of the security of the data system, provided that the PI is not used or subject to further unauthorized disclosure.

Notification Obligation. Any Entity to which the statute applies shall, when it becomes aware of a breach of the security of the system, conduct in good faith a reasonable and prompt investigation to determine the likelihood that PI has been or will be misused. If the investigation determines that the misuse of PI about a WY resident has occurred or is reasonably likely to occur, the Entity shall give notice as soon as possible to the affected WY resident.

Third-Party Data Notification. An Entity that maintains computerized data that includes PI on behalf of another Entity shall disclose to the Entity for which the information is maintained any breach of the security of the system as soon as practicable following the determination that PI was, or is reasonably believed to have been, acquired by an unauthorized person.

The Entity that maintains the data on behalf of another Entity and Entity on whose behalf the data is maintained may agree which Entity will provide any required notice, provided only a single notice for each breach of the security of the system shall be required. If agreement regarding notification cannot be reached, the Entity who has the direct business relationship with the resident of WY shall provide the required notice.

Timing of Notification. Notice shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.

Personal Information Definition. The first name or first initial and last name of a person in combination with one or more of the following data elements when the data elements are not redacted:

- Social Security Number;
- Driver license number;
- Account number or credit card number or debit card number in combination with any security code, access code or password that would allow access to a financial account of the person;
- Tribal identification card;
- Federal or state government-issued identification card;

[Effective July 1, 2015:]

- Shared secrets or security tokens that are known to be used for data based authentication;
- A username or email address, in combination with a password or security question and answer that would permit access to an online account;

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	• A birth or marriage certificate; • Medical information, meaning a person's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; • Health insurance information, meaning a person's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the person or information related to a person's application and claims history; • Unique biometric data, meaning data generated from measurements or analysis of human body characteristics for authentication purposes; • An individual taxpayer identification number. PI does not include information, regardless of its source, contained in any federal, state or local government records or in widely distributed media that are lawfully made available to the general public. **Notice Required.** Notice shall be clear and conspicuous and shall include, at a minimum, • a toll-free number that the individual may use to contact the person collecting the data, or his agent; and from which the individual may learn the toll-free contact telephone numbers and addresses for the major credit reporting agencies; [Effective July 1, 2015 • The types of personal identifying information that were or are reasonably believed to have been the subject of the breach; • A general description of the breach incident; • The approximate date of the breach of security, if that information is reasonably possible to determine at the time notice is provided; • In general terms, the actions taken by the individual or commercial entity to protect the system containing the personal identifying information from further breaches; • Advice that directs the person to remain vigilant by reviewing account statements and monitoring credit reports; and • Whether notification was delayed as a result of a law enforcement investigation, if that information is reasonably possible to determine at the time the notice is provided Notice may be provided by one of the following methods: • Written notice; or • Electronic mail notice. **Substitute Notice Available.** If the Entity demonstrates that the cost of providing notice would exceed $10,000 for WY-based Entities, and $250,000 for all other Entities operating but not based in Wyoming; that the affected class of subject persons to be notified exceeds 10,000 for WY-based Entities and 500,000 for all other businesses operating but not based in WY; or the person does not have sufficient contact information. Substitute notice shall consist of all of the following: • Conspicuous posting of the notice on the Internet, the World Wide Web or a similar proprietary or common carrier electronic system site of the person collecting the data, if the person maintains a

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.

	public Internet, World Wide Web or a similar proprietary or common carrier electronic system site; and • Notification to major statewide media. The notice to media shall include a toll-free phone number where an individual can learn whether or not that individual's personal data is included in the security breach. **Exception: Compliance with Other Laws.** • **Certain Financial Institutions.** Any financial institution as defined in 15 U.S.C. § 6809 or federal credit union as defined by 12 U.S.C. § 1752 that maintains notification procedures subject to the requirements of 15 U.S.C. § 6801(b)(3) and 12 C.F.R. pt. 364 App. B or pt. 748 App. B, is deemed to be in compliance with the statute if the financial institution notifies affected WY customers in compliance with the requirements of 15 U.S.C. § 6801 through 6809 and 12 C.F.R. pt. 364 App. B or pt. 748 App. B. • **[Effective July 1, 2015] HIPAA.** A covered entity or business associate that is subject to and complies with the Health Insurance Portability and Accountability Act, and the regulations promulgated under that act, 45 C.F.R. Parts 160 and 164, is deemed to be in compliance if the covered entity or business associate notifies affected Wyoming customers or entities in compliance with the requirements of the Health Insurance Portability and Accountability Act and 45 C.F.R. Parts 160 and 164. **Other Key Provisions:** • **Delay for Law Enforcement.** The notification required by the statute may be delayed if a law enforcement agency determines in writing that the notification may seriously impede a criminal investigation. • **AG Enforcement.** The state AG may bring an action in law or equity to address any violation of this section and for other relief that may be appropriate to ensure proper compliance with this section, to recover damages, or both.

This chart is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. The most current copy of this chart and additional information on Perkins Coie's Privacy and Security Group can be found at http://www.perkinscoie.com/privacy_security.