Revised October 2026

Security Breach Notification Chart

Ashurst Perkins Coie's Privacy 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. If you experience a breach and are in need of legal counsel, please **CONTACT THE INCIDENT RESPONSE TEAM** and we will get back to you as soon as possible. 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

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

Alabama

Ala. Stat. § 8-38-1 *et seq.*

Alabama S.B. 318 (signed into law March 28, 2018)

Effective June 1, 2018

[BACK TO TABLE OF CONTENTS]

Application: A person or commercial entity (collectively, Entity) that acquires or uses sensitive personally identifying information.

Security breach definition: The unauthorized acquisition of data in electronic form containing sensitive personally identifying information.

- Good-faith acquisition of sensitive personally identifying information by an employee or agent of an Entity is not a security breach, provided that the information is not used for a purpose unrelated to the business or subject to further unauthorized use.
- A security breach also does not include the release of a public record not otherwise subject to confidentiality or nondisclosure requirements, nor does it include any lawful, investigative, protective, or intelligence activity of a law enforcement or intelligence agency of the state, or a political subdivision of the state.

Notification obligation: Notice is required to affected AL residents if the Entity determines that, as a result of a breach of security, personal information has been acquired by an unauthorized person and is reasonably likely to cause substantial harm.

Notification to consumer reporting agencies: If an Entity is required to notify more than 1,000 AL residents of a breach, the Entity shall also notify without unreasonable delay all nationwide consumer credit reporting agencies of the timing, distribution, and content of the notices to AL residents.

Attorney general/agency notification: If the number of individuals requiring notice exceeds 1,000, the Entity must notify the attorney general as expeditiously as possible and without unreasonable delay, and within 45 days once it is determined that a breach has occurred and is reasonably likely to cause substantial harm to affected individuals. Written notice must include:

- A synopsis of the events surrounding the breach
- The number of affected individuals in AL
- 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
- The name, address, telephone number, and email address of the employee or agent of the Entity from whom additional information may be obtained about the breach

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 shall provide notices to the attorney general 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 contract with the Entity whereby the third-party agent agrees to handle required notifications.

Timing of notification: Notice shall be made as expeditiously as possible and without unreasonable delay, taking into account the time necessary to conduct an investigation, and within 45 days of discovering that a breach has occurred and is reasonably likely to cause substantial harm to affected individuals.

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	Personal information definition: An AL resident's first name or first initial and last name, in combination with one or more of the following data elements: • Social Security number; • Tax identification number; • Driver's license number or state identification card number, passport number, military identification number, or other unique identification number issued on a government document used to verify the identity of a specific individual; • Account number, credit card number, or debit card number in combination with any required security code, access code, password, expiration date, or PIN, that is necessary to access the financial account or to conduct a transaction that will credit or debit the financial account; • Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; • An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual; or • A username or email address, in combination with a password or security question and answer that would permit access to an online account affiliated with the Entity that is reasonably likely to contain or is used to obtain sensitive personally identifying information Personal information does not include information about an individual that is lawfully made public by a federal, state, or local government record or widely distributed media. Personal Information does not include information that is truncated, encrypted or otherwise rendered unusable, unless the encryption key or other credential necessary to render the information usable has also been compromised. **Notice required:** Notice may be provided by one of the following methods: • Written notice; or • Email notice Notice must contain, at a minimum: • The date, estimated date, or estimated date range of the breach • A description of the PI that was acquired • A general description of the actions taken by the Entity to restore the security and confidentiality of the PI • A general description of the steps the affected individuals can take to protect themselves from identity theft • Contact information for the Entity where individuals can inquire about the breach **Substitute notice available:** If the Entity demonstrates (1) excessive cost (greater than $500,000 or excessive relative to the Entity's resources);

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	(2) more than 100,000 persons are affected, or (3) the Entity does not have sufficient contact information to provide notice. Substitute notice shall include both of the following:
	• Conspicuous posting of the notice on the website of the Entity if the Entity maintains one, for a period of 30 days; and
	• Notice to major print and broadcast media, including major media in urban and rural areas where the affected individuals reside
	Exception: Compliance with other laws:
	• An Entity is exempt from this chapter if it:
	  • Is subject to or regulated by (1) federal laws, rules, regulations, procedures, or guidance *or* (2) state laws, rules, regulations, procedures, or guidance that are at least as thorough as the notice requirements in this law; and
	  • Maintains procedures pursuant to those requirements;
	  • Provides notice to consumers pursuant to those requirements; and
	  • Timely provides notice to the attorney general when the number of affected individuals exceeds 1,000
	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 or national security, and the law enforcement agency has submitted a written request for the delay. The law enforcement agency may revoke the delay as of a specified date or extend the delay, if necessary.
	• Government entities are subject to the Act as well and must provide notice in line with the provisions of the law.
	• **Attorney general enforcement:** The attorney general has exclusive authority to bring an action for civil penalties under the 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

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 doing business, 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.

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: An Entity to which the statute applies shall disclose the breach to each AK resident whose PI was subject to the breach.

- Notification is not required if, after an appropriate investigation and after written notification to the state attorney general, the Entity determines that there is not a reasonable likelihood that harm 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 nationwide consumer credit reporting agencies of 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 an Entity experiences a breach of the security of PI on an AK resident that the Entity does not own or license, 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: Notification 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 or more of the following data elements:

- Social Security number;
- Driver's license number or state 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	• Account number, 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; or • 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 to the most recent address the Entity has; • 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) **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 **all** 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 website 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 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

Arizona

Ariz. Rev. Stat. § 18-551 *et seq.*

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

Effective December 31, 2006

H.B. 2154 (signed into law April 11, 2018, Chapter 177)

Effective August 3, 2018

H.B. 2146 (signed into law March 29, 2022, Chapter 81)

Effective June 27, 2022

[BACK TO TABLE OF CONTENTS]

Application: Any person or entity (collectively, Entity) that conducts business in AZ and that owns, maintains, or licenses unencrypted and un-redacted computerized PI.

Security breach definition: An unauthorized acquisition and access that materially compromises the security or confidentiality of unencrypted and un-redacted computerized PI maintained by an Entity as part of a database of PI regarding multiple individuals.

- 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 unauthorized disclosure.

Notification obligation: Any Entity that owns or licenses the PI shall notify the individuals affected within 45 days after its determination that there has been a security breach.

- An Entity is not required to disclose a breach of the system if the Entity, an independent third-party forensic auditor, or a law enforcement agency, after a reasonable investigation, determines that a breach has not resulted in or is not reasonably likely to result in substantial economic loss to affected individuals.

Attorney general notification: If an Entity is required to notify more than 1,000 AZ residents, the Entity shall notify the attorney general and the Director of the Arizona Department of Homeland Security, in writing, in a form prescribed by rule or order of the attorney general, or by providing a copy of the individual notification.

Notification to consumer reporting agencies: If an Entity is required to notify more than 1,000 AZ residents, the Entity shall also notify the three largest nationwide consumer reporting agencies.

Third-party data notification: If an Entity maintains unencrypted and un-redacted computerized PI that the Entity does not own or license, the Entity shall notify, as soon as possible, the owner or licensee of the information, and cooperate with the owner or the licensee of the information. Cooperation shall include sharing information relevant to the breach The Entity that maintains 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 within 45 days after the Entity's determination that there has been a security breach.

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:

- Social Security number;
- Number on a driver's license issued pursuant to § 28-3166 or number on a nonoperating identification license issued pursuant to § 28-3165;
- Financial account number or credit 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	• A private key that is unique to an individual and that is used to authenticate or sign an electronic record; • An individual's health insurance identification number; • Information about an individual's medical or mental health treatment or diagnosis by a health care professional; • Passport number; • Individual's taxpayer identification number or an identity protection personal identification number issued by the IRS; and • Unique biometric data generated from a measurement or analysis of human body characteristics to authenticate an individual when the individual accesses an online account 2. An individual's username or email address, in combination with a password or security question and answer, that allows 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 or widely distributed media. **Notice required:** *Generally:* Notice may be provided by one of the following methods: • Written notice; • Telephonic notice, if made directly with the affected individuals and not through a pre-recorded message; or • Email notice, if the Entity has email addresses for the individuals subject to the notice The notice shall include at least the following: • The approximate date of the breach; • Type of PI included in the breach; • The toll-free telephone numbers and addresses of the three largest credit reporting agencies; and • The toll-free number, address, and website for the FTC or any federal agency that assists consumers with identity theft matters *For online account credentials:* If the breach involves only online account credentials and no other PI, the Entity may comply with this section by providing the notification in an electronic or other form that directs the individual whose PI has been breached to promptly change their password and security question or answer, as applicable, or to take other steps that are appropriate to protect the online account and all other online accounts for which the individual uses the same username and email address and password or security question or answer. *For email account credentials:* For the breach of credentials to an email account furnished by the Entity, the Entity may comply with this section by providing notification by another method described in this subsection or by providing clear and conspicuous notification delivered to the individual online when connected to the online account from an IP address or online location from which the Entity knows the individual customarily accesses the 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	The Entity satisfies the notification requirement with regard to the individual's account with the person by requiring the individual to reset their password or security question and answer for that account, if the person also notifies the individual to change the same password or security question and answer for all other online accounts for which the individual uses the same username or email address and password or security question or answer. **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: • A written letter to the attorney general that demonstrates the facts necessary for substitute notice; and • Conspicuous posting of the notice on the website of the Entity, if the Entity maintains one **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:** The provisions of the statute do not apply to a covered entity or business associate as defined under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) or a charitable fund-raising foundation or nonprofit corporation whose primary purpose is to support a specified covered entity, if they comply with applicable provisions of HIPAA. • **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. **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 within 45 days after the law enforcement agency determines that notification will no longer impede the investigation. • **Attorney general enforcement:** A knowing and willful violation of this section is an unlawful practice pursuant to ARS 44-1522. The attorney general may impose a civil penalty for a violation of this article not to exceed the lesser of $10,000 per affected individual or the total amount of economic loss sustained by affected individuals, but the maximum civil penalty from a breach or series of related breaches may not exceed $500,000.

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

Arkansas

Ark. Code § 4-110-101 *et seq.*

(Go to the Arkansas Code Search page, Title 4, Subtitle 7, Chapter 110)

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

Effective August 12, 2005

H.B. 1943 (signed into law on April 15, 2019, Act 1030)

Effective July 23, 2019

[BACK TO TABLE OF CONTENTS]

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

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: An Entity to which the statute applies shall disclose any 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's license number or state identification card number;
- Account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account;
- 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); or
- Biometric data (data generated by automatic measurements of an individual's biological characteristics) and any other unique biological characteristics of an individual if used to uniquely authenticate the individual's identity for access to a system of account

Notice required: Notice may be provided by one of the following methods:

- Written notice; 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	• Email 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 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 website of the Entity, if the Entity maintains one; and • Notification to statewide media **Attorney general notification:** If the affected class of persons to be notified exceeds 1,000, the Entity must disclose the breach to the attorney general. Notice must be provided at the same time the Entity notifies the affected class, or 45 days after it determines there is a reasonable likelihood of harm to individuals, whichever is first. **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. • Attorney general enforcement. • **Records retention:** An Entity must retain a copy of the determination of the breach and any supporting documentation for five years from the date the breach was determined.

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

California

Cal. Civ. Code § 1798.29; **1798.82 *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

A.B. 1130 (signed into law on October 11, 2019)

Effective January 1, 2020

S.B. 446 (signed into law October 3, 2025)

Effective January 1, 2026

[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.

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: An Entity to which the statute applies shall disclose any breach of the security of the system following discovery or notification to any CA resident (1) whose unencrypted PI was, or is reasonably believed to have been, acquired by an unauthorized person, or (2) whose encrypted PI was, or is reasonably believed to have been, acquired by an unauthorized person and the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person and the Entity that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that PI readable or useable.

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: Disclosure to affected individuals must be made within 30 calendar days of discovery or notification of the data breach. The entity may delay the disclosure to accommodate 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. Submission of the sample copy of the notification to the attorney general must be made within 15 calendar days of notifying affected consumers of the security breach.

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's license number or state identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual;

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	• Account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to 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 information in an individual's application and claims history, including any appeals records); • 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); • Biometric data generated from measurements or technical analysis of human body characteristics (*e.g.*, fingerprint, retina, or iris image) used to authenticate a specific individual; or • Genetic data (data that results from the analysis of a biological sample of an individual, or from another source enabling equivalent information to be obtained, and concerns genetic material) 2. Username 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:** *Generally:* 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) 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;

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	• A general description of the breach incident, if that information is possible to determine at the time the notice is provided; and • 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 state identification card number See below re credit monitoring information, if offered. 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; and • Advice on steps that the person whose information was breached may take to protect him or herself 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.) *For online account credentials:* 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 username or email address and password or security question or answer *For email account credentials:* 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 via methods otherwise permitted, or via 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. **Credit monitoring services**: If the person or business offers credit monitoring or identity theft prevention and mitigation services, the services must be provided at no cost to the affected person for not less than 12 months, and all information necessary to take advantage of the offer must be provided in the notice. This provision applies only if the person providing notice was the source of the breach and if the breach exposed or may have exposed PI involving Social Security numbers or covered forms of government identification (driver's license, state identification card numbers, tax identification number, passport number, military identification number, 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	other unique identification number issued on a government document commonly used to verify the identity of a specific individual). **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 email addresses for the subject persons; • Conspicuous posting for at least 30 days of the notice on the Entity's website, if the Entity maintains one (meaning providing a link to the notice on the home page or first significant page after entering the website 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. **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 individual notice content requirements in this state law if it has complied with the individual notice content requirements in Section 13402(f) of the Health Information Technology for Economic and Clinical Health Act (HITECH). Covered entities are not otherwise exempt from the statute's requirements. **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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

Colorado

Colo. Rev. Stat. § 6-1-716

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

Effective September 1, 2006

H.B. 18-1128 (signed into law on May 29, 2018)

Effective September 1, 2018

[BACK TO TABLE OF CONTENTS]

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

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 a purpose unrelated to the lawful operation of the business or is not subject to further unauthorized disclosure.

Notification obligation: An Entity that owns or licenses the affected PI 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.

Attorney general notification: If notice is provided to more than 500 CO residents, the Entity must provide notice to the attorney general not later than 30 days after the date of determination that the breach occurred.

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 nationwide consumer reporting agencies of the anticipated date of the notification and the approximate number 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, but not later than 30 days after the date of determination that the breach occurred, 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:
(1) 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;
- Student, military, or passport ID number;
- Driver's license number or other 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	• Medical information; • Health insurance identification number; or • Biometric data (2) Username or email address, in combination with a password or security question that would permit access to an online account; or (3) Account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to that 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 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) For incidents that involve login credentials of an email account furnished by the Entity, notice may not be given to that email address, but may be given by clear and conspicuous notice delivered to the resident online when connected to the account from an IP address or online location from which the Entity knows the resident customarily accesses the account. The notice must include: • The date, estimated date, or estimated date range of the breach; • Type of PI subject to the unauthorized acquisition; • Information the resident can use to contact the Entity to inquire about the security breach; • The toll-free telephone numbers, addresses, and websites of the major credit reporting agencies and the Federal Trade Commission; and • A statement that the resident can obtain information from the Federal Trade Commission and the credit reporting agencies about fraud alerts and security freezes For a breach of online account credentials, *in addition to* the information above, the notice must direct the consumer to promptly change his or her password or question and answer, or to take other steps appropriate to protect the online account with the covered Entity and all other online accounts for which the person whose PI has been breached uses the same username or email address and password or security question or answer. **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:

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	• 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 website 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. • **Attorney general enforcement:** The attorney general 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

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

S.B. 472 (signed into law June 4, 2018)

Effective October 1, 2018

H.B. 5310 (signed into law June 16, 2021)

Effective October 1, 2021

S.B. 1058 (Signed into law June 26, 2023)

Effective October 1, 2023

[BACK TO TABLE OF CONTENTS]

Application: Any person (Entity) that owns, licenses, or maintains computerized data that includes PI of Connecticut residents.

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: An 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 the Entity reasonably determines that the breach will not likely result in harm to the individuals whose PI has been acquired or accessed.

Notification obligation to attorney general: Any Entity that is required under the statute to notify CT residents of any breach of security shall provide notice of the breach of security to the attorney general not later than the time notice is provided to the residents.

Third-party data notification: If an Entity maintains 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, but not later than 60 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.

- If additional residents whose information has been breached or reasonably believed to be breached is identified more than 60 days after discovery, the Entity shall notify as expediently as possible.

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:

- Social Security number;
- Driver's license number or state identification card number;
- Credit card number, or debit card number;
- Financial account number, in combination with any required security code, access code, or password that would permit access to such financial account;
- Taxpayer identification number;
- Identity protection personal identification number issued by the IRS;
- Passport number, military identification number or other identification number issued by the government that is commonly used to verify identity;

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	• Medical information regarding individual medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; • Health insurance policy number or subscriber identification number, or any unique identifier used by a health insurer to identify the individual; • Biometric information consisting of data generated by electronic measurements of an individual's unique physical characteristics used to authenticate or ascertain the individual's identity, such as a fingerprint, voice print, retina or iris image; or • Precise geolocation data OR (2) username or email address in combination with a password or security question and answer that would permit access to an online account (name not required). 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: *Generally:* • Written notice; • 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) *Online account credentials:* Notice may be provided in electronic or other form directing the resident to promptly change any password or security question or to take other appropriate steps to protect the affected online account and all other online accounts for which the resident uses the same username or email address and password or security question and answer. *Email account credentials:* An Entity that furnishes an email account shall not provide notice to the email account that was breached if the Entity cannot reasonably verify the affected person's receipt of that notification. In such event, notice should be provided by another method described in this section or clear and conspicuous notice delivered to the resident when they are online and connected to the account from an IP address or online location from which the person knows the resident customarily accesses the account. **Credit monitoring services:** The Entity who owns or licenses the affected PI shall offer to each resident whose Social Security number or taxpayer identification number 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 24 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.

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	Substitute notice available: If the Entity demonstrates in the notice to the 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 persons, 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 affected persons; • Conspicuous posting of the notice on the website 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. • **HIPAA and Health Information Technology for Economic and Clinical Health Act (HITECH):** Compliance with HIPAA and HITECH is deemed compliance with the statute, provided that the Entity provides notice to the state attorney general no later than when notice is provided to residents and offers identity theft protection to those whose Social Security Number or taxpayer identification number was breached. **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. • **Attorney general enforcement:** The attorney general may seek direct damages and injunctive relief. Any civil penalties collected for failure to comply may be deposited into the privacy protection guaranty and enforcement account. • **Public disclosure exception:** All documents, materials, and information provided in response to an investigative demand issued pursuant to section 42-110d(c) shall be exempt from public disclosure under section 1-210(a) provided the attorney general may make such documents, materials or information available to third parties in furtherance of such 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

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

House Substitute 1 for HB 180 (signed into law August 17, 2017)

Effective April 14, 2018

H.B. 381 (approved September 2, 2026)

[BACK TO TABLE OF CONTENTS]

Application: Any person, legal or commercial entity, or government agency who conducts business in DE (collectively, Entity) and who owns or licenses computerized data that includes PI.

Security breach definition: The unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of PI. The unauthorized acquisition of encrypted data is not a breach, unless such unauthorized acquisition includes, or is reasonably believed to include, an encryption key that could render the PI readable or useable.

- 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 an unauthorized purpose or subject to further unauthorized disclosure.

Notification obligation: An Entity to which the statute applies shall provide notice of any breach of security following determination of the breach of security to any resident of DE whose PI was breached or is reasonably believed to have been breached.

- Notification is not required if after an appropriate investigation the Entity reasonably determines that the breach of security is unlikely to result in any harm to the individuals whose PI has been breached.

Attorney general notification: If the number of DE residents to be notified exceeds 500 residents, the Entity 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: 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 determination of the breach of security. Cooperation includes sharing with the owner or licensee information relevant to the breach.

Timing of notification: Without unreasonable delay but not later than 60 days after determination of the breach of security.

- If the Entity cannot, through reasonable diligence, identify within 60 days that the PI of certain DE residents was included in a breach of security, the Entity must provide notice as soon as practicable after determining that the breach of security included the PI of those residents. The Entity must also provide notice of the breach of security to the attorney general within 60 days after determining the breach, unless substitute notice has been or is provided within 60 days.

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:

- Social Security number;
- Driver's license number or state or federal identification card number;
- Account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to a resident'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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	• Passport number; • Username or email address, in combination with a password or security question and answer that would permit access to an online account; • Medical history, medical treatment by a healthcare professional, diagnosis of mental or physical condition by a health care professional, or deoxyribonucleic acid (DNA) profile; • Health insurance policy number, subscriber identification number, or any other unique identifier used by a health insurer to identify the person; • Unique biometric data generated from measurements or analysis of human body characteristics for authentication purposes; or • An individual taxpayer identification number 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; • 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) or if the person's primary means of communication with the resident is by electronic means *For email account credentials:* 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 via methods otherwise permitted, or by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an IP address or online location from which the person knows the resident customarily accesses the account. **Credit monitoring services:** If the breach of security includes Social Security numbers, the Entity shall offer to each resident whose Social Security number was affected, credit monitoring services at no cost to such resident for a period of one year. The Entity shall provide all information necessary for such resident to enroll in such services and shall include information on how such resident can place a credit freeze on his or her credit file. **Substitute notice available:** If the Entity demonstrates that the cost of providing notice will exceed $75,000, or that the number of DE residents to be notified exceeds 100,000, 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 website of the Entity, if the Entity maintains 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	• Notice to major statewide media, including newspapers, radio, television, and publications, on the major social media platforms of the person providing notice; and • Notice of the breach of security to the attorney general **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:** An Entity is deemed in compliance with the timing requirements for providing breach notification if: o It is regulated by state or federal law, including HIPAA or GLBA; o It maintains procedures for a breach of security pursuant to requirements established by its primary or functional state or federal regulator; and o It notifies affected DE residents in accordance with the maintained procedures. **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. • **Attorney general 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

District of Columbia

D.C. Code § 28-3851 *et seq.*

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

Effective July 1, 2007

Council Bill 23-0215 (signed into law March 26, 2020)

Effective June 17, 2020

[BACK TO TABLE OF CONTENTS]

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

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.
- Acquisition of personal information of an individual that the Entity reasonably determines, after a reasonable investigation and consultation with the Office of the Attorney General and federal law enforcement agencies, will likely not result in harm to the individual, is not a breach.

Notification obligation: An Entity to which the statute applies, and that discovers a breach of the security system shall promptly notify any D.C. 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 nationwide consumer reporting agencies, 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.

Attorney general/agency notification: If 50 or more residents are affected, the Entity must notify the attorney general as expeditiously as possible and without unreasonable delay, and no later than when individual notice is sent.

The notice must include:

- Name and contact information of the person or entity reporting the breach;
- Name and contact information of the person or entity that experienced the breach;
- The nature of the breach of the security of the system;
- Types of personal information compromised by the breach;
- Number of District residents affected by the breach;
- Cause of the breach, including the relationship between the person or entity that experienced the breach and the person responsible for the breach, if known;
- Remedial action taken, to include steps taken to assist District residents affected by 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	• Date and time frame of the breach, if known; • Address and location of corporate headquarters, if outside of the District; • Any knowledge of foreign country involvement; and • Sample of the notice to be provided to District residents **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:** 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:** (1) An individual's first name, first initial and last name, or any other personal identifier, which, in combination with any of the following data elements, can be used to identify a person or the person's information: • Social security number, Individual Taxpayer Identification Number, passport number, driver's license number, District of Columbia identification card number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual; • Account number, credit card number or debit card number, or any other number or code or combination of numbers or codes, such as an identification number, security code, access code, or password, that allows access to or use of an individual's financial or credit account; • Medical information; • Genetic information and deoxyribonucleic acid profile; • Health insurance information, including a policy number, subscriber information number, or any unique identifier used by a health insurer to identify the person that permits access to an individual's health and billing information; • Biometric data of an individual generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voice print, genetic print, retina or iris image, or other unique biological characteristic, that is used to uniquely authenticate the individual's identity when the individual accesses a system or account; or • Any combination of data elements included in the above bullet points that would enable a person to commit identity theft without reference to a person's first name or first initial and last name or other independent personal identifier (2) Username or email address in combination with a password, security question and answer, or other means of authentication, or any combination 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	data elements included in the above bullet points, that permits access to an individual's email account. PI shall not include 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 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) Notice shall include: • Categories of information accessed • Contact information for Entity making notification • Contact information for consumer reporting agencies, the FTC, and Office of the Attorney General **Credit monitoring services:** When the breach is reasonably believed to include a social security number or taxpayer identification number, the Entity shall offer to each resident whose social security number or tax identification number was released identity theft protection services at no cost to such resident for at least 18 months. **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 email addresses for the subject persons; • Conspicuous posting of the notice on the website of the Entity, if the Entity maintains one; and • Notice to major local and, if applicable, national media **Exception: Compliance with other laws:** An Entity that maintains procedures for a breach notification system under the GLBA, HIPAA, or HITECH, and provides notice in accordance with such Acts, and any rules, regulations, guidance and guidelines thereto, to each affected resident in the event of a breach, shall be deemed to be in compliance with the law with respect to the notification of affected individuals. The Entity shall, in all cases, provide written notice of the breach of the security of the system to the Office of the Attorney General. **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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	• **Attorney general enforcement:** The attorney general may seek direct damages and injunctive relief. • **Private right of action:** Any D.C. 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

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

*S.B. 262 (signed into law June 6, 2023)

Effective July 1, 2024

[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 PI (collectively, Entity).

- For notice requirements, Entity includes governmental entities.

An entity that has been contracted to maintain, store, or process PI on behalf of an Entity or governmental entity (Third-Party Agent).

Security breach definition: The unauthorized access of data in electronic form containing PI.

- 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: An 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 five years

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 FL. Written notice must include:

- A synopsis of the events surrounding the breach at the time notice is provided
- The number of individuals in FL 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 email address of the employee or agent of the Entity from whom additional information may be obtained about the breach

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

Notification to consumer reporting agencies: If notice is required to more than 1,000 FL residents, the Entity shall also notify, without unreasonable delay, all nationwide consumer reporting agencies of the timing, distribution, and content of the notices.

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	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 affected individuals:** Notice must be made as expeditiously as practicable and without unreasonable delay, but no later than 30 days after the determination of a breach or reasons to believe a breach occurred, 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 to restore the reasonable integrity of the data system that was breached. The Entity may receive 15 additional days to provide notice to Affected Individuals if good cause for delay is provided in writing to the Department within 30 days after determination. **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: o Social Security number; o Driver's license or state identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity; o 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; o Information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or o Health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual o **[as of July 1, 2024]** An individual's biometric information or genetic information; or o **[as of July 1, 2024]** Any information regarding an individual's geolocation.

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	• A username 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 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: • Written notice sent to the mailing address of the individual in the records of the Entity; or • Email notice sent to the individual's email address in the Entity's records 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 PI that the Entity maintained about the individual **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 website, 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 an 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 (1) in the amount of $1,000 for each day the breach goes undisclosed for up to 30 days and, thereafter, $50,000 for each 30-day period or portion therefore for up to 180 days; or (2) 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	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. A 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. • **No private cause of action:** There is no private cause 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

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.

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 nationwide consumer reporting agencies of the timing, distribution, and content of the notices.

Third-party data notification: Any person or business that maintains computerized data on behalf of an Entity that includes PI 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: 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's license or state identification card number;
- Account number, credit card number, 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	• 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; • Telephone 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 email addresses for the individuals to be notified; • 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:** 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

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 commercial or legal entity, 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).

Security breach definition: Any unauthorized access to and acquisition of unencrypted or un-redacted 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: An Entity 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, shall notify the owner or licensee of the PI of any security breach immediately following discovery of the breach.

Timing of notification: 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.

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	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's license number or state 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 **all** the following: • Email notice when the Entity has email addresses for the subject persons; • Conspicuous posting of the notice on the Entity's website, if the Entity maintains one; and • Notification to major 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	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. • Attorney general 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

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.

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.

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's license number or state 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

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 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)

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	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 website 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. **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 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

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

S.B. 1624 (signed into law August 9, 2019)

Effective January 1, 2020

[BACK TO TABLE OF CONTENTS]

Application: Any 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.

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.

Attorney general notification: Any Entity required to notify more than 500 Illinois residents must provide notice to the attorney general of the breach. Notice must include:

- A description of the nature of the breach of security;
- The date of the breach;
- The number of Illinois residents affected by such incident at the time of notification; and
- Any steps the Entity has taken or plans to take relating to the incident

If the date of the breach is unknown at the time the notice is sent to the attorney general, the Entity shall send the attorney general the date 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 steps taken or planned relating to the breach.

Timing of notification: In the most expedient time possible and without unreasonable delay, but in no event later than when the data collector provides notice to consumers pursuant to this Section.

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:

- Social Security number;
- Driver's license number or state identification card number;
- Account number, 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;

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	• 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); or • 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 (2) Username 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. PI does not include information that is encrypted or redacted where the keys to provide access to the information have not also been obtained. **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 • For breaches involving username/email and password/security questions **only,** in "electronic or other form" **Contents of notice:** *Generally:* For a breach of PI other than username/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 IL residents affected by the breach. *Online account credentials only:* Notice may be provided in electronic or other form directing the IL resident whose PI has been breached to promptly change his or her username 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 username 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

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	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, if the Entity has email addresses for the subject persons; • Conspicuous posting of the notice on the Entity's website, if the Entity maintains one; and • Notification to major statewide media or, 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**: 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 five business days of notifying the Secretary. **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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

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

H.E.A, No. 1341 (signed into law March 18, 2022)

S.B. 17 (signed into law March 13, 2024)

Effective July 1, 2024

[BACK TO TABLE OF CONTENTS]

Application: Any individual or legal entity (collectively, Entity) that owns or licenses computerized data that includes PI.

- State agencies are separately covered by § 4-1-11, which has similar individual notification requirements.

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 (1) has not been compromised or disclosed, and (2) 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: An Entity shall disclose the breach to affected IN residents 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.

Notice must be provided to whose unencrypted PI was or may have been acquired by an unauthorized person and those whose encrypted PI was or may have been acquired by an unauthorized person with access to the encryption key.

Attorney general notification: If the Entity makes such a disclosure, the database 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 nationwide 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, but not more than 45 days after the discovery of the breach, and consistent with any measures necessary to determine the scope of the breach and restore the integrity of the system.

Personal information definition: (1) A Social Security number that is not encrypted or redacted, (2) 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	• A driver's 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; or (3) information collected by an adult oriented website operator, or their designee, under **IC 24-4-23**. 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 website 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

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	the Entity and the Entity complies with the Entity's information privacy, security policy, or compliance plan. **Other key provisions:** • **Attorney general 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 attorney general. 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

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

2018 S.F. 2177 (signed into law April 10, 2018)

Effective July 1, 2018

[BACK TO TABLE OF CONTENTS]

Application: Any individual, government, 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: An Entity to which the statute applies shall give notice of the breach of security following discovery, 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: An Entity required to notify more than 500 IA residents must give written notice to the director of the consumer protection division of the attorney general's office. Notice or receipt of notice must be provided within five 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, 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, un-redact, or otherwise read the data elements have also been obtained through the breach of security:

- Social Security 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	• Driver's license number or other unique identification number created or collected by a government body; • Account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to 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: • Email notice when the Entity has email addresses for the affected IA residents; • Conspicuous posting of the notice or a link to the notice on the Entity's website, if the Entity maintains one; and • Notification to major 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	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 a 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. • **HIPAA and HITECH:** This statute does not apply to an Entity that is subject to and complies with the regulations promulgated pursuant to the Title II, subtitle F of the Health Insurance Portability and Accountability Act (HIPAA) and Title XIII, subtitle D of the Health Information Technology for Economic and Clinical Health Act (HITECH). **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. • Attorney general 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

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, legal or government entity (collectively, Entity) that conducts business in KS and that owns or licenses computerized data that includes PI.

Security breach definition: Any unauthorized access to and acquisition of unencrypted or un-redacted 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: An 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 nationwide consumer reporting agencies 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's license number or state identification card number; or
- Account number, 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:

- Written notice; 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	• 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 website, if the Entity maintains one; and • Notification to major statewide media **Exceptions:** • **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. • **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 **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. • **Attorney general enforcement.** Allows the state attorney general (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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

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, 2015KY Rev. Stat. §61.931 ***ET SEQ.***

Effective January 1, 2015

[BACK TO TABLE OF CONTENTS]

Application: "Information Holder" is defined as any person or business entity that conducts business in Kentucky (collectively, Entity).

- Obligations for state agencies *and private parties that receive, collect or maintain* data from state agencies are different and more detailed than those described below. *See* KY Rev. Stat. §61.931 et seq.

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 KY 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: An Entity to which the statute applies must, upon discovery or notification of breach in the security system, notify any KY resident whose unencrypted information 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 more than 1,000 persons, the Entity shall also notify, without unreasonable delay, all nationwide consumer reporting agencies 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.

- Special note that under the state agency provisions in §61.932-.933, a private company contracting with a state agency 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. The contracting agency or institution bears the responsibility of notifying any affected individuals and the state attorney general.

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.

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's license number; or
- Account number, credit card number, or debit card number in combination with any required security code, access code, 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	password that would permit access to an individual's financial account Obligations under these statutes apply only to unencrypted, unredacted computerized data. **Notice required:** Notice may be provided by one of the following methods: • Written notice; or • 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: • Email notification if the Entity has email 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:** • **Federal laws:** The provisions of this statute do 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 of 1996 (HIPAA) • **State agencies:** This statute does not apply to any KY agency, or any KY local governments or political subdivisions. (*But see* KY Rev. Stat. §61.931 *et seq*.) **Other key provisions:** • **Delay for law enforcement:** An 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.

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

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

S.B. 361 (signed into law May 16, 2018, Act 382)

Effective August 1, 2018

[BACK TO TABLE OF CONTENTS]

Application: Any individual, any legal entity that conducts business in LA, or any agency that owns or licenses computerized data that includes PI (collectively, Entity).

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: An Entity shall 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 no reasonable likelihood of harm to LA residents. The Entity shall retain a copy of the written determination and supporting documentation for five years and provide a copy to the attorney general upon request.

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 attorney general shall be timely if received within 10 days of distribution of notice to LA citizens.

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: In the most expedient time possible and without unreasonable delay, but not later than 60 days from discovery of the breach, consistent with any measures necessary to determine the scope of the breach, prevent further disclosures, and restore the reasonable integrity of the data system. When notification is delayed by law enforcement request or due to a determination by the Entity that measures are necessary to determine the scope of the breach, prevent further disclosures, and restore the reasonable integrity of the data system, the Entity shall provide the attorney general the reasons for the delay in writing within the 60-day notification period. Upon receipt of the written reasons, the attorney general shall allow a reasonable extension of time to provide the consumer notification.

Personal information definition: The first name or first initial and last name of a LA resident 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's license number or state 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	• Account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; • Passport number; or • Biometric data: "Biometric Data" means data generated by automatic measurements of an individual's biological characteristics, such as fingerprints, voice print, eye retina or iris, or other unique biological characteristic that is used by the owner or licensee to uniquely authenticate an individual's identity when the individual accesses a system or 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 $100,000, 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 notification, when the Entity has email addresses for the subject persons; • Conspicuous posting of the notification on the Entity's website, 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 that 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 the 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

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	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 attorney general shall be timely if received within 10 days of distribution of notice to LA citizens. Each day that notice is not received by the state attorney general shall be deemed a separate 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. 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

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

L.D. 696 (signed into law June 28, 2019, Chapter 512)

Effective September 19, 2019

[BACK TO TABLE OF CONTENTS]

Application: Any individual, or other legal or government entity, or any information broker (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) that maintains computerized data that includes PI (collectively, Entity).

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: An Entity shall give notice of the 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 attorney general.

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, the nationwide consumer reporting agencies of 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: If notice is not delayed due to law enforcement, notification must be made no more than 30 days after becoming aware of the breach and identifying its scope. 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 seven business days after a law enforcement agency determines 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:

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	• Social Security number; • Driver's license number or state identification card number; • Account number, 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 PI does not include information from third-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 website, 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. **Exception: Compliance with other laws:** • An entity that complies with the security breach notification requirements of rules, regulations, procedures or guidelines established pursuant to Maine or federal law is deemed to be in compliance with the requirements as long as the law, rules, regulations or guidelines provide for notification procedures at least as protective as the notification requirements outlined above. **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

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	than seven business days after a law enforcement agency determines that the notification will not compromise a criminal investigation. • **Attorney general enforcement:** Enforced by state attorney general 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

Maryland

Md. Code Com. Law § 14-3501 *et seq.*

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

Effective January 1, 2008

H.B. 974 (signed into law May 4, 2017)

Effective January 1, 2018

H.B. 962 (signed into law May 29, 2022)

Effective October 1, 2022

[BACK TO TABLE OF CONTENTS]

Application: Any business entity, whether or not organized to operate at a profit, (collectively, Entity) that owns, maintains, or licenses computerized data that includes PI of an individual residing in 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 that 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 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. If, after the investigation is concluded, the Entity determines that the breach of the security of the system creates a likelihood that PI has been or will be misused, the business shall notify the individual of the breach.

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, and the notice shall include, at a minimum:

- The number of affected individuals residing in the State;
- A description of the breach of the security of a system, including when and how it occurred;
- Any steps the business has taken or plans to take relating to the breach of the security of a system; and
- The form of notice that will be sent to affected individuals and a sample notice

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 PI of MD residents 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 practicable but not later than 45 days 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.

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	Timing of notification: As soon as reasonably practicable, but no later than 45 days after the business concludes the investigation, 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:** (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 the data elements are not encrypted, redacted, or otherwise protected by another method that renders the information unreadable or unusable: • Social Security number, individual taxpayer identification number, passport number, or other identification number issued by the federal government; • Driver's license number or state identification card number; • Account number, credit card number, or debit card number, in combination with any required security code, access code, or password, that permits access to an individual's financial account; • Health information, including information about an individual's mental health; • Health insurance policy or certificate number or health insurance subscriber identification number, in combination with a unique identifier used by an insurer or an employer that is self-insured, that permits access to an individual's health information; or • Biometric data of an individual generated by automatic measurements of an individual's biological characteristics such as a fingerprint, voice print, genetic print, retina or iris image, or other unique biological characteristic, that can be used to uniquely authenticate the individual's identity when the individual accesses a system or account; or • Genetic information of an individual (2) A username or email address in combination with a password or security question and answer that permits access to an individual's email account. "Encrypted" means the protection of data in electronic or optical form using an encryption technology that renders the data indecipherable without an associated cryptographic key necessary to enable decryption of the data. PI does not include (1) publicly available information that is lawfully made available to the general public from federal, state, or local government records; (2) information that an individual has consented to have publicly disseminated or listed; or (3) information that is disseminated or listed in accordance with the federal Health Insurance Portability and Accountability Act of 1996 (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

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	• Email 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 *Generally:* Except for breaches involving loss of information that permits access to an email account only, 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 website addresses for (1) the Federal Trade Commission and (2) the state attorney general, along with a statement that the individual can obtain information from these sources about steps the individual can take to avoid identity theft *For email account credentials only:* the Entity may provide notice in electronic or other form that directs the individual whose PI has been breached promptly to: • Change the individual's password and security question or answer, as applicable; or • Take other steps appropriate to protect the email account with the business and all other online accounts for which the individual uses the same username or email and password or security question or answer The notification may be given by a clear and conspicuous notice delivered to the individual online while the individual is connected to the affected email account from an IP address or online location from which the business knows the individual customarily accesses the account but otherwise may not be given to the individual by sending notification by email to the email account affected by the breach. **Substitute notice available:** If the Entity demonstrates that 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 website, if the Entity maintains a website; and • Notification to major print or broadcast media in geographic areas where the individuals affected by the breach likely reside **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

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	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. • An Entity or affiliate of the Entity that is in compliance with the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) shall be deemed to be in 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 or jeopardize homeland or national security. Notification shall be given as soon as reasonably practicable but no later than seven days after the law enforcement agency determines that it will not impede a criminal investigation and will not jeopardize homeland or national security if (1) the original 45 day period has already elapsed, or (2) the end of the original 45 day period, or (3) seven days after the law enforcement agency determines that it will not impede a criminal investigation and will not jeopardize homeland or national security. • Attorney general 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

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

H.B. 4806 (signed into law on January 10, 2019)

Effective April 11, 2019

[BACK TO TABLE OF CONTENTS]

Application: A natural person, legal entity, or any MA government agency (collectively, Entity) that owns, licenses, maintains, or stores data that includes PI about a resident 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.
- **Note:** Notification obligations apply to a Breach of Security ***OR*** acquisition or use without authorization.

Notification obligation: An Entity that owns or licenses the data shall provide notice to the affected residents, when the Entity knows or has reason to know of (1) a breach of security, **OR** (2) that the PI of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose.

Attorney general/state agency notification. When notice is provided to a MA resident, notice must be provided to both the state attorney general and the director of Consumer Affairs and Business Regulation.

The notice shall include, but not be limited to:

- the nature of the breach of security or unauthorized acquisition or use;
- the number of residents of MA affected by such incident at the time of notification;
- the name and address of the person or agency that experienced the breach of security;
- the name and title of the person or agency reporting the breach of security, and their relationship to the person or agency that experienced the breach of security;
- the type of person or agency reporting the breach of security;
- the person responsible for the breach of security, if known;
- the type of personal information compromised, including, but not limited to, social security number, driver's license number, financial account number, credit or debit card number or other data;
- whether the person or agency maintains a written information security program; and
- any steps the person or agency has taken or plans to take relating to the incident, including updating the written information security program

A person who experienced a breach of security shall file a report with the attorney general and the director of consumer affairs and business regulation certifying their credit monitoring services comply with the law's requirements

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	for providing credit monitoring to individuals if social security numbers are affected. Note that both agencies currently promulgate online forms containing the required information. • Upon receipt of notice, the director of consumer affairs and business regulation shall report the incident publicly on its website and make available electronic copies of the sample notice sent to consumers on its website. • 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. **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 (1) knows or has reason to know of a breach of security or (2) 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 the owner or licensor. Such Entity shall cooperate with the owner or licensor of such PI. Cooperation shall include, but not be limited to (1) informing the owner or licensor of the breach of security or unauthorized acquisition or use, (2) the date or approximate date of such incident and the nature thereof, and (3) 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. Entities cannot delay notification “on the grounds that the total number of residents affected is not yet ascertained.” **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’s 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.

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 Ashurst Perkins Coie’s Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	Notice required: Notice provided to the resident 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. It must, however, include: • The resident's right to obtain a police report; • How a resident may request a security freeze and the necessary information to be provided when requesting the security freeze; • That there shall be no charge for a security freeze; and • Mitigation services to be provided pursuant to this chapter If the person or agency that experienced a breach of security is owned by another person or corporation, the notice to the consumer shall include the name of the parent or affiliated corporation. 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) **Credit monitoring:** An Entity that experiences an incident requiring notice and involving social security numbers shall provide credit monitoring services at no cost to such affected residents for a period of not less than 18 months. The Entity shall provide all information necessary for enrollment and shall include information on how the resident may place a security freeze. **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 the Entity's website, if the Entity maintains one; and • Publication in or broadcast through media that provide 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 if (1) notice is provided to affected Massachusetts residents in accordance with the maintained or required procedures when a breach occurs; and (2) the Entity also notifies the attorney general and the director of the office of consumer affairs and business regulation. **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 attorney general, in writing, thereof

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	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. • **Attorney general 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

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

H.B. 6406 (signed into law December 28, 2018)

Effective January 20, 2020

[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.

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 that owns or licenses data including MI residents shall provide notice of the breach to each resident of MI if (1) the resident's unencrypted and unredacted PI was accessed and acquired by an unauthorized person or (2) 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 MI residents, the Entity shall, after notifying those residents, notify each nationwide consumer reporting agency without unreasonable delay of 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's license number or state personal identification card number; or
- Demand deposit or other financial account number, or credit card or debit card number, in combination with any required security 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	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 (1) the notice is not given in whole or in part by use of a recorded message, (2) 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 3 business days after the initial attempt to provide telephonic notice; or • Written notice sent electronically to the recipient if (1) the recipient has expressly consented to receive electronic notice, (2) 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 (3) 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 website, if the Entity maintains one; and • Notification to major statewide media, which notice shall include a telephone number or website address that a person may use to obtain additional assistance and information

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	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 website 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. • **Insurers:** Entities subject to or regulated under Michigan's insurance code are exempt from the state's data breach notification statute and instead will be governed by HB 6491/Public Act 690 of 2018, which goes into effect January 20, 2021. **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.

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	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. • Attorney general enforcement. • Provides that Entities may deliver notice pursuant to an agreement with another Entity, if the agreement does not conflict with MI 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

Minnesota

Minn. Stat. § 325E.61 and 325E.64

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 (collectively, Entity), and that owns or licenses data that includes PI.

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: An 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 nationwide consumer reporting agencies 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's license number or state identification card number; or
- Account number, credit card number, or debit card number, in combination with any required security code, access code, or password that would permit access to 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 with the individual is by electronic means, or if the notice provided is

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	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 <u>all</u> of the following: • Email notice, if the Entity has email addresses for the 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. **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. • Attorney general 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

Mississippi

Miss. Code § 75-24-29

(Follow link to Lexis, scroll to Title 75, Chapter 24)

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 PI 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 that 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 PI 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's license number or state identification card number; or
- Account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to 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 persons;

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	• 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 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. • **Attorney general 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

Missouri

Mo. Rev. Stat. § 407.1500

H.B. 62

Effective August 28, 2009

[BACK TO TABLE OF CONTENTS]

Application: Any individual, legal or commercial or government entity (collectively, Entity) that owns or licenses PI of residents 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.

- 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 nationwide consumer reporting agencies 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 attorney general'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, 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:

- Social Security number;
- Driver's license number or other unique identification number created or collected by a government body;
- Account number, credit card number, or debit card number in combination with any required security code, access code, 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	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 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 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: • Email notice when the Entity has an email address for the affected consumer; • Conspicuous posting of the notice or a link to the notice on the Entity's website, if the Entity maintains one; and • Notification to major 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	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:** • **Regulated entity:** 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. • **Financial institution:** A financial institution that is (1) 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 (2) subject to and in compliance with the National Credit Union Administration regulations in 12 C.F.R. Part 748; or (3) 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 attorney general 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

Montana

Mont. Code § 2-6-1501 *et seq*, 30-14-1701 *et seq*., 33-19-321

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

S.B. 50 (signed into law April 24, 2023)

Effective October 1, 2023

[BACK TO TABLE OF CONTENTS]

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

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: An 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).

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.

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;
- 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;

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	• Medical record information as defined in § 33-19-104 (PI that (1) relates to an individual's physical or mental condition, medical history, medical claims history, or medical treatment; and (2) 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 email addresses for the subject persons **and** one of the following: • Conspicuous posting of the notice on the Entity's website, 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 the 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

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, 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.

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 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 notification: If notice of a security breach to NE residents is required, the Entity shall also, not later than the time when notice is provided to the NE 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:

(1) 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 otherwise altered by any method or technology in such a manner that the name or data elements are unreadable:

- Social Security number;
- Driver's license number or state 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	• Account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to 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 (2) A username or email address, in combination with a password or security question and answer, that would permit access to an online account. 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 website, 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 3 consecutive weeks; • Conspicuous posting of the notice on the Entity's website, if it 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	• 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. • **Attorney general enforcement:** The attorney general 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

Nevada

Nev. Rev. Stat. § **603A.010 *et seq.*, 242.183**

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

Effective October 1, 2005 and January 1, 2006:

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: An Entity to which the statute applies shall disclose any breach of the security of the system data 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 nationwide consumer reporting agencies of the timing and content of the notice.

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 that PI 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's license number, driver authorization card number or identification card number;
- Account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account;
- A medical identification number or a health insurance identification number; or
- A username, unique identifier, or email 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's license or driver authorization card number, or the last four digits of an identification card number or publicly available information

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	that is lawfully 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 email addresses for the 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 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. • **Attorney general enforcement:** If the state attorney general 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 or she 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 PI 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	• **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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

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, or any form of entity or government agency (collectively, Entity) doing business in NH that owns or licenses computerized data that includes PI.

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 determines that misuse of PI 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 PI 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 nationwide consumer reporting agencies of the timing, distribution, and 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 that has primary regulatory authority over such trade or commerce. All other Entities shall notify the state attorney general. 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 PI 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.

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's license number or other government identification number; or
- Account number, credit card number, or debit card number in combination with any required security code, access code, 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	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 email addresses for the affected individuals; • Conspicuous posting of the notice on the Entity's website, 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. **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.

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	• Attorney General 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

New Jersey

N.J. Stat. § 56:8-161 *et seq.*

A. 4001 (signed Sept. 22, 2005)

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

Senate Bill No. 52 (signed into law May 10, 2019)

Effective September 1, 2019

[BACK TO TABLE OF CONTENTS]

Application: Any government, or other entity, however organized and whether or not organized to operate at a profit, that conducts business in NJ (collectively, Entity), that compiles or maintains computerized records that include PI.

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: An 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 nationwide consumer reporting agencies 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 last name linked with any one or more of the following data elements:

- Social Security number;
- Driver's license number or state identification card number;
- Account number, credit card number, or debit card number in combination with any required security code, access code, 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	password that would permit access to an individual's financial account; or • Username, email address, or any other account holder identifying information, in combination with any password or security question and answer that would access to an online 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) • For breaches involving online account credentials only, in "electronic or other form" o Except for breaches involving credentials for an email account, which must be provided via written notice or via online delivery when the customer is connected to the online account from an IP address or online location from which the business or public entity knows the customer customarily accesses the account. **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 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 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

New Mexico

N.M. STAT. 57-12C-1 *et seq.*

H.B. 15 (signed into law April 6, 2017)

Effective June 16, 2017

[BACK TO TABLE OF CONTENTS]

Application: Any person that owns or licenses elements that include PI of a New Mexico resident (collectively, Entity).

Security breach definition: Unauthorized acquisition of unencrypted computerized data, or of encrypted computerized data and the confidential process or key used to decrypt the encrypted computerized data, that compromises the security, confidentiality, or integrity of PI maintained by a person.

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

Notification obligation: An Entity to which the statute applies shall notify each NM resident whose PI is reasonably believed to have been subject to a security breach.

- Notification to NM residents is not required if, after an appropriate investigation, the Entity determines that the security breach does not give rise to a significant risk of identity theft or fraud.

Notification to consumer reporting agencies: If more than 1,000 NM residents are to be notified as a result of a single security breach, the Entity shall also notify major consumer reporting agencies in the most expedient time possible, and no later than 45 calendar days, except if delayed notification is permitted to determine the scope of the breach or for law enforcement investigation purposes.

Attorney general/agency notification: If more than 1,000 NM residents are to be notified as a result of a single security breach, the Entity shall also notify the Office of the Attorney General of the number of NM residents that received notification pursuant and shall provide a copy of the notification that was sent to affected residents within 45 calendar days following discovery of the security breach, except if delayed notification is permitted to determine the scope of the breach or for law enforcement investigation purposes.

Third-party data notification: Any business that is licensed to maintain or possess computerized data containing PI of a New Mexico resident that the business does not own or license shall notify the owner or licensee of the security breach in the most expedient time possible, but not later than 45 calendar days following discovery of the breach, except if delayed notification is permitted to determine the scope of the breach or for law enforcement investigation purposes. However, notification to the owner or licensee of the PI is not required if, after an appropriate investigation, the business determines that the security breach does not give rise to a significant risk of identity theft or fraud.

Timing of notification: Notification shall be made in the most expedient time possible, but not later than 45 calendar days following discovery of the security breach. Notification may be delayed as necessary to determine the scope of the security breach and restore the 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 one or more of the following data elements that relate to the individual, when the data elements are not protected through encryption or redaction or otherwise rendered unreadable or unusable:

- Social Security 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	• Driver's license number; • Government-issued identification number; • Account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to a person's financial account; or • Biometric data "Personal information" does not include information lawfully obtained from publicly available sources or from federal, state or local government records lawfully made available to the general public. **Notice required:** The notice shall include: • The name and contact information of the notifying person; • A list of the types of PI that are reasonably believed to have been the subject of a security breach, if known; • The date of the security breach, the estimated date of the breach, or the range of dates within which the security breach occurred, if known; • A general description of the security breach incident; • The toll-free telephone numbers and addresses of the major consumer reporting agencies; • Advice that directs the recipient to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach; and • Advice that informs the recipient of the notification of the recipient's rights pursuant to the federal Fair Credit Reporting Act The notice shall be provided by one of the following methods: • United States mail; or • Electronic notification, if the Entity primarily communicates with the NM resident by electronic means or if the notice provided is consistent with the requirements of 15 U.S.C. Section 7001 (E-Sign Act) **Substitute notice available:** If the Entity demonstrates that the cost of providing notification would exceed $100,000; or that the number of residents to be notified exceeds 50,000; or that the Entity does not have a physical address or sufficient contact information for the residents to be notified. Substitute notice shall consist of all of the following: • Sending electronic notification to the email address of those residents for whom the Entity has a valid email address; • Posting notification of the security breach in a conspicuous location on the website of the Entity, if the Entity maintains one; and • Sending written notification to the Office of the Attorney General and major media outlets in New Mexico

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	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 the statute is deemed to be in compliance if the Entity notifies affected consumers in accordance with its policies in the event of a security breach. **Exception: Compliance with other laws:** • Statute does not apply to an Entity subject to the federal Gramm-Leach-Bliley Act or the federal Health Insurance Portability and Accountability Act of 1996. **Other key provisions:** • **Delay for law enforcement:** Notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. • **Attorney general enforcement:** The attorney general may bring an action for an injunction and 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

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

S. 5575B (signed into law July 25, 2019)

Effective October 23, 2019

S. 02659 (signed into law December 21,2024)

S. 00804 (signed into law February 14, 2025)

[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) that conducts business in New York State and that owns or licenses computerized data that includes **private information.**

Security breach definition: Unauthorized access to or acquisition of, or access to or acquisition without valid authorization, of computerized data that compromises the security, confidentiality, or integrity of private information maintained by a business.

In determining whether information has been **accessed,** or is reasonably believed to have been accessed, Entities may consider, among other factors, indications that the information was viewed, communicated with, used, or altered by a person without valid authorization or by an unauthorized person.

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 access to or acquisition of private information 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 within 30 days of 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, accessed or acquired by a person without valid authorization.

Notice to affected persons is not required if the exposure of private information was an inadvertent disclosure by persons authorized to access private information, and the Entity reasonably determines such exposure will not likely result in misuse of such information, or financial harm to the affected persons or emotional harm in the case of unknown disclosure of online credentials. This determination must be documented in writing and maintained for at least five years. If more than 500 NY residents are affected, the Entity shall provide the written determination to the state attorney general within ten days after the determination.

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 the 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 department of state consumer protection board, and the division of state police as to the timing, content and distribution of the notices and approximate number 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	affected persons and shall provide a copy of the template notice sent to affected persons. The state AG's website has a form to be used for notifications. • **Special note for HIPAA covered entities:** Any Covered Entity required to provide notification of a breach, including breach of information that is not "private information" as defined herein, to the Secretary of Health and Human Services pursuant to HIPAA or the HITECH Act, shall provide such notification to the state attorney general within five days of notifying the Secretary. **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, provided that such notification shall be made within 30 days 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, provided that such notification shall be made within 30 days after the breach has been discovered, 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 that, because of name, number, personal mark, or other identifier, can be used to identify such natural person. **Private information definition:** Personal information consisting of: (1) Any information in combination with any one or more of the following data elements, when either the data element or the combination of personal information plus the data element is not encrypted, or is encrypted with an encryption key that has also been accessed or acquired: • Social Security number; • Driver's license number or non-driver identification card number; • Account number, credit or debit card number, if circumstances exist wherein such number could be used to access an individual's financial account without additional identifying information, security code, access code, or password; or • Biometric information, meaning data generated by electronic measurements of an individual's unique physical characteristics, such as fingerprint, voice print, retina or iris image, or other unique physical representation or digital representation of biometric data which are used to authenticate or ascertain the individual's identity; or (2) A username or email address in combination with a password or security question and answer that would permit access to an online 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. • NY's statute uses the term "private information" the same way most statutes use "personal information," and separately defines "personal information" to mean all identifiable information about a person. 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	latter term is used only to require that notices include *all* types of personal *and* private information that has been exposed. **Notice required:** Notice shall include: • Contact information for the Entity making the notification; • The telephone numbers and websites of the relevant state and federal agencies that provide information regarding security breach response and identity theft prevention and protection information; and • A description of the categories of information that were, or are reasonably believed to have been, accessed or acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so accessed or 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 attorney general 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 email addresses for the subject persons, except if the breached information includes an email address in combination with a password or security question and answer that would permit access to the online account, in which case the Entity shall instead provide clear and conspicuous notice delivered to the consumer online when the consumer is connected to the online account from an internet protocol address or from an online location which the Entity knows the consumer customarily uses to access the online account; • Conspicuous posting of the notice on the Entity's website, if the Entity maintains one; and • Notification to major 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	Exception: Compliance with other laws: If notice of the breach of the security of the system is made pursuant to any of the following laws, nothing in this statute shall require separate notice to affected individuals, but notice must still be provided to the regulators noted above and the consumer reporting agencies. • Regulations promulgated pursuant to Title V of the federal Gramm-Leach-Bliley Act (GLBA) • Regulations implementing the Health Insurance Portability and Accountability Action of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) • Part 500 of Title 23 of the Code of the State of New York (NY DFS Cybersecurity Regulation) • Any other data security rules and regulations of, and the statutes administered by, any official department, division, commission, or agency of the federal or New York state government **Other key provisions:** • **Delay for law enforcement:** The notification required by this 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. • **Attorney general enforcement:** The attorney general 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

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 legal entity, however organized and whether or not organized to operate at a profit, but not including any government or governmental subdivision or agency (collectively, Entity) that owns or licenses PI of residents of NC or that conducts business in NC and 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: If 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 nationwide consumer reporting agencies 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 attorney general'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.

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 PI 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;
- Driver's license, state identification card, or passport numbers;
- Checking account numbers;
- Savings account numbers;
- Credit card numbers;
- Debit card 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	• PINs; • 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 website addresses for the Federal Trade Commission and the state attorney general'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

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	• Electronic notice, for those persons for whom it 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) **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 email addresses for the subject persons; • Conspicuous posting of the notice on the Entity's website, if the Entity maintains one; and • Notification to major statewide media **Exception: Compliance with other laws:** • **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 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. • **Attorney general enforcement:** Civil and criminal penalties are 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

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.

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 databases 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: 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 that exceeds 250 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: 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;
- An account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to 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
- The individual's digitized or other electronic signature

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	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 Entity 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 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 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 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:** • **Interagency guidance:** 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. • **HIPAA:** A covered 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. • Attorney general 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

Ohio

Ohio Rev. Code, 1347.12, 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.

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.

- Good faith acquisition of PI by an employee or agent of the Entity for the purposes of the Entity is not a breach, provided that the personal information is not used for an unlawful purpose or subject to further unauthorized disclosure.
- Acquisition of personal information pursuant to a search warrant, subpoena, or other court order, or pursuant to a subpoena, order, or duty of a regulatory state agency, is not a breach.

Notification obligation: Any Entity to which the statute applies shall disclose any 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 notifies more than 1,000 residents of OH, the Entity shall notify, without unreasonable delay, all nationwide consumer reporting agencies of the timing, distribution, and content of the notice.

- This requirement does not apply to HIPAA covered entities.

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: 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 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's license number or state identification card number; 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	• Account number, credit card number, or debit card number in 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 types 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 notice would exceed $250,000, that the affected class of subject residents to whom 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 website, 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 notice 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 3 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	• Conspicuous posting of the disclosure or notice on the Entity's website 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:** • **Financial institution:** A financial institution, trust company, or credit union or any affiliate thereof 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. • **Attorney general enforcement:** The attorney general 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

Oklahoma

24 Okla. Stat. § 161 *et seq.*, § 74-3113.1

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

Effective November 1, 2008

S.B. 626 (signed into law May 28, 2025)

Effective January 1, 2026.

Applies to breaches determined or notified on or after January 1, 2026.

[BACK TO TABLE OF CONTENTS]

Application: Any corporations, or any other legal or government 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 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 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.

Attorney general notification: Any Entity that experiences a breach of the security system shall disclose to the attorney general within 60 days after providing notice to impacted individuals for any breach of the security system that affects 500 individuals. (Entities that are credit bureaus have a higher threshold, 1,000 or more residents). Notice will be kept confidential.

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: 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's license or other unique identification number created or collected by a government entity; or
- Account number, credit card number, debit card number, unique electronic identifier, or routing code in combination with any required

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	expiration date, security code, access code, or password that would permit access to financial accounts. • Biometric data such as fingerprint, retina, iris image, or other unique physical or digital biometric data PI shall not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public. **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 email addresses for the members of the affected class of residents; • Conspicuous posting of the notice on the Entity's website 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:** The following entities are deemed to be in compliance with the statute if they provide notice to the attorney general as otherwise required: • **Interagency guidance:** A financial institution that complies with the notification requirements prescribed by the Gramm-Leach-Bliley Act and the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice. • **Covered entity:** An entity that complies with the notification requirements prescribed by the Oklahoma Hospital Cybersecurity Protection Act of 2023 or the Health Insurance Portability and Accountability Act of 1996 (HIPAA). • **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. **Penalties:** The state attorney general 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

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	that are discovered in a single investigation. Civil penalties shall be based upon the magnitude of the breach, the extent to which the behavior of the individual or entity contributed to the breach, and any failure to provide the notice as required by this section. - Safeguards to entities that use reasonable safeguards and provide notice, exempting them from civil penalties. - An entity that provides notice but does not use reasonable safeguards is not subject to additional civil penalties but is liable for actual damages and a $75,000 civil penalty. **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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

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

S.B. 1551 (signed into law on March 16, 2018)

Effective June 2, 2018

S.B. 684 (signed into law on May 24, 2019)

Effective January 1, 2020

[BACK TO TABLE OF CONTENTS]

Application: Any individual or legal 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, licenses, maintains, stores, manages, collects, processes, acquires or otherwise possesses PI in the course of the Entity's business, vocation, occupation or volunteer activities. This does not include any person or entity that contracts with the Entity to maintain, store, manage, process or otherwise access PI for the purpose of, or in connection with, providing services to or on behalf of the Entity.

Security breach definition: Unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of PI maintained or possessed 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: An Entity to which the statute applies shall give notice of the breach of security 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 notifies more than 1,000 individuals under this section, the Entity shall notify, without unreasonable delay, all nationwide consumer reporting agencies of the timing, distribution, and content of the notification. The Entity shall include the police report number, if available, in its notification to the consumer reporting agencies.

Attorney general notification: The entity must provide notice to the attorney general, either in writing or electronically, if the number of OR 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 another person shall notify the other person of any breach of security as soon as practicable, but not later than 10 days after discovering the breach of security or having a reason to believe that the breach of security occurred. That person must also notify the attorney general in writing or electronically if the number of residents affected exceeds 250 or cannot be determined, unless the Entity has already notified the attorney general.

Timing of notification: The disclosure shall be made in the most expedient manner possible and without unreasonable delay, but not later than 45 days after discovering or receiving notice of the breach. In providing the notice, the Entity shall take reasonable 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.

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	Personal information definition: (1) 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: • Social Security number; • Driver's 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, 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, or any other information or combination of information that a person reasonably knows or should know would permit access to the consumer's financial account; • 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; or • 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 (2) A username or other means of identifying a consumer for the purpose of permitting access to the consumer's account, together with any other method necessary to authenticate the username or means of identification. 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 providing the notice; • Contact information for national consumer reporting agencies; 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	• 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) **Credit monitoring services:** If an Entity offers credit monitoring or identity theft prevention services without charge, the Entity may not require the affected individual to provide a credit or debit card number or accept another service offered by the Entity for free. If services are offered for a fee, the Entity must separately, distinctly, clearly, and conspicuously disclose in the offer that the person will charge the consumer a fee. The entity must require compliance with these terms from any company offering services on the entity's behalf. **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 website, if the Entity maintains a website; and • Notification to major statewide television and newspaper media **Exception: Compliance with other laws:** In each of the following cases, Oregon's notification requirements do not apply, except that any person claiming one of these exemptions and notifying more than 250 Oregon residents must provide a copy of the individual notice and any notice to any primary or functional regulator, to the Oregon Attorney General: • **Primary regulator:** Personal information that is subject to, and an Entity that complies with the notification requirements or breach of security procedures that the person's primary or functional federal regulator adopts, promulgates or issues in rules, regulations, procedures, guidelines or guidance. • **Gramm-Leach-Bliley Act:** An Entity 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/HITECH:** An Entity that complies with regulations promulgated under HIPAA or the HITECH Act. • **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

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	as thorough disclosure requirements for a breach of security of PI than that provided by this section. **Other key provisions:** • **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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

Pennsylvania

73 Pa. Stat. § 2301 *et seq.*

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

Effective June 20, 2006

S.B. 696 (signed into law Nov. 3, 2022, Act. No. 151)

Effective May 2, 2023

S.B. 824 (signed into law June 28, 2024, Act No. 33)

Effective September 26, 2024

[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.

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 to any individual whose principal mailing address, as reflected in the computerized data that is maintained, stored, or managed by the Entity, is in PA and 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 key.

Notification to attorney general: Any Entity required to notify more than 500 Pennsylvania residents must concurrently provide notice to the attorney general of the breach. Notice must include:

- The organization name and location;
- The date of the breach of the security of the system;
- A summary of the breach incident;
- An estimated total number of individuals affected by the breach; and
- An estimated total number of Pennsylvania affected by the breach

Notification to consumer reporting agencies: When an Entity provides notification under this act to more than 500 persons at one time, the Entity shall also notify, without unreasonable delay, all nationwide consumer reporting agencies of the timing, distribution, and number of notices.

Credit monitoring services and providing free credit report: If a breach of security has occurred and the Entity reasonably believes that the data accessed includes an individual's first name and last name or an individual's first initial and last name, in combination with (1) Social Security number, (2) bank account number, or (3) driver's license or state ID number, the Entity must also:

- Offer affected individuals credit monitoring services at no cost for a period of 1 year
- Assume all costs and fees in providing the affected individuals access to one independent credit report from a consumer reporting agency if the individual is not eligible to obtain an independent credit

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	report from a consumer reporting agency for free under 15 U.S.C. § 1681 If these requirements are triggered, the no-cost services must be described in the individual notification. **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 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's license number or state identification card number issued in lieu of a driver license; • Account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; • Medical Information in the possession of a State agency or State agency contractor; • Health Insurance Information; or • Username or email address in combination with a password or security questions and answers 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 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 a website 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 *For online account credentials:* Notice may be provided in electronic form that directs the individual to promptly change his or her password and security question or answer, or to take other appropriate steps to protect the online account with the entity or other online accounts involving the same login credentials.

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	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 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 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. **Exception: Entities subject to Insurance Data Security Act:** An Entity that is subject to the requirements of the Pennsylvania Insurance Data Security Act (40 PA. C.S. CH. 45) is exempt from notice requirements to the attorney general. **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 national or homeland security. • **Attorney general enforcement:** The attorney general 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

Puerto Rico

10 L.P.R.A. ST § 4051 *et seq.*

(Scroll down to Ten, Subtitle 3, Chapter 310)

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

Effective January 5, 2006

(Scroll down to Ten, Subtitle 3, Chapter 310)

[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 database 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 database 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 databases 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 nonextendable term of 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 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 to access it there is no need to use a special cryptographic code:

- Social Security number;
- Driver's license number, voter 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 of 1996 (HIPAA);
- Tax information; or
- Work-related evaluations

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	Neither the mailing nor the residential address is included in the PI, nor is information that is in a public document and is available to 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 a website for people to use to obtain information or assistance. Notice may be provided by one of the following methods: • Written notice; or • Authenticated electronic means according to 15 U.S.C. § 7001 (E-Sign 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 $100,000 or the number of persons exceeds 100,000, the entity shall issue the notice through the following steps: • Prominent display of an announcement to that respect at the entity's premises, on the website 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 them 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 toward that sector. **Exception:** Conflict with preexisting institutional security policies. 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. **Penalties:** The Secretary may impose fines from $500 up to $5,000 for each violation. The fines provided in this section do not affect the rights of the consumers to initiate actions or claims for damages before a competent court.

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

Rhode Island

R.I. Gen. Laws § 11- 49.3-4 *et seq.*

H.B. 5684 signed into law June 27, 2023

Effective June 27, 2023

[BACK TO TABLE OF CONTENTS]

Application: A municipal agency, state agency, individual, business or legal 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.
- Note that the notification obligation applies to a breach of security of the system ***or*** any disclosure of PI.

Notification obligation: Any Entity to which the statute applies shall provide notification of (1) any disclosure of PI ***or*** (2) any breach of the security of the system, that 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.

- Where affected employees are represented by a labor union through a collective bargaining agreement, a state or municipal agency employer shall also notify the collective bargaining agent of the breach.

Attorney general notification: If more than 500 RI residents are to be notified, the Entity shall notify the attorney general as to the timing, content, and distribution of the notices and the approximate number of affected individuals.

- State and municipal agencies must also report cybersecurity incidents to the RI state police within 24 hours.

Credit reporting agency notification: In the event that more than 500 RI residents are to be notified, the Entity shall notify the major credit reporting agencies as to the timing, content, and distribution of the notices and the approximate number of affected individuals.

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.

For state and municipal Entities, notice must be given no later than 30 calendar days.

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's license number, state identification card number, or tribal identification number;
- Account number, credit card number, or debit card number in combination with any required security code, access code, password,

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	or personal identification number that would permit access to an individual's financial account; • Medical or health insurance information; or • Email 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 encrypted if it is acquired in combination with any key, security code, or password that would permit access to the encrypted data. 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; 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: • A general and brief description of the incident, including how the security breach occurred and the number of affected individuals; • The type of information that was subject to the breach; • The date of breach, estimated date of breach, or the date range within which the breach occurred; • The date that the breach was discovered; • A clear and concise description of any remediation services offered to affected individuals including toll free numbers and websites to contact (1) credit reporting agencies; (2) remediation service providers; and (3) the attorney general; and • A clear and concise description of the consumer's ability to file or obtain a police report, how the consumer can request a security freeze and the necessary information to be provided when requesting the security freeze, and any fees that 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 email addresses for the subject persons; • Conspicuous posting of the notice on the Entity's website 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	• Notification to major statewide media **Credit monitoring services:** State and municipal Entities must provide remediation services for five years for adults 18 years and older, and up to the age of 18 and not less than two years for those under 18. **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 of the system. • **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

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

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, commercial or legal entity, government or governmental subdivision or agency conducting business in SC (collectively, Entity) and owning or licensing 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 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 nationwide consumer reporting agencies 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’s license number or state identification card number issued instead of a driver license;
- Financial account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to a resident’s financial account; 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 Ashurst Perkins Coie’s Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	• Other numbers or information that may be used to access a 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 email addresses for the 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 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 SC resident whose information was accessible by reason of the breach, the amount to be decided by the Department of Consumer Affairs.

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	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 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

South Dakota

S.D. CODE 22-40-20 *et seq.*

South Dakota S.B. 62 (signed into law March 21, 2018)

Effective July 1, 2018

[BACK TO TABLE OF CONTENTS]

Application: Any person or business that conducts business in South Dakota, and that owns or licenses computerized personal or protected information of residents of SD (Entity).

Security breach definition: The unauthorized acquisition of unencrypted computerized data or encrypted computerized data and the encryption key by any person that materially compromises the security, confidentiality, or integrity of personal or protected information.

- Good-faith acquisition of personal or protected information by an employee or agent of an Information Holder is not a security breach, provided that the information is not used for a purpose unrelated to the business or subject to further unauthorized use.

Notification obligation: Any Entity that discovers or is notified of a breach of system security must notify affected individuals.

- Notice is not required if, following appropriate investigation and notification to the attorney general, the Entity reasonably believes the incident will not result in harm to affected individuals. The Information Holder shall document this determination in writing and keep record of this documentation for three years.

Attorney general notification: If the number of affected individuals exceeds 250 residents, the Entity must notify the attorney general.

Notification to consumer reporting agencies: The Entity must notify, without unreasonable delay, all nationwide consumer reporting agencies.

Timing of notification: Notice must be given no later than 60 days from when the Entity discovers or is notified of a breach.

Personal information definition: SD's statute covers both "personal information" and "protected information."

"Personal Information" means a person'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's license number or any other unique identification number created or collected by a government body;
- Account number, credit card number, or debit card number in combination with any required security code, access code, password, routing number, PIN, or any additional information that is necessary to access the financial account;
- Health information as defined in 45 CFR 160.103 (HIPAA); or
- An identification number assigned to a person by the person's employer in combination with any required security code, access code, password, or biometric data generated from measurements or analysis of human body characteristics for authentication purposes

The term does not include information that is lawfully made available to the general public from federal, state, or local government records or information that has been redacted, or otherwise made unusable.

"Protected information" includes:

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	• A username or email address, in combination with a password, security question answer, or other information that permits access to an online account; and • Account number or credit and debit card number, in combination with any required security code, access code, or password that permits access to a person's financial account **Notice required:** Notice may be provided by one of the following methods: • Written notice; • Electronic notice, if the electronic notice is consistent with the requirements for electronic records and signatures set forth in 15 U.S.C. § 7001 (E-Sign Act), or if the information holder's primary method of communication with the SD resident has been by electronic means **Substitute notice available:** Substitute notice is acceptable if notification will exceed $250,000, the affected class of persons to be notified exceeds 500,000 persons, or the Entity does not have sufficient contact information and the notice consists of each of the following: • Email notice, if the Entity has the affected individual's email address; • Conspicuous posting of the notice on the website of the Entity, if it has a website; and • Notification to statewide media **Exception: Own notification policy:** An Entity that maintains its own notification procedure as part of its information security policy, and the policy is consistent with the timing requirements of the Act, is considered in compliance with the notification requirements of this Act if it notifies affected persons in accordance with its internal policy **Exception: Compliance with other laws:** • **Federal law:** An Entity subject to or regulated by federal laws, rules, regulations, procedures, or guidance (including the Gramm-Leach-Bliley Act and HIPAA) is considered in compliance with the Act as long as the Entity maintains procedures pursuant to the federal law requirements and provides notice to consumers pursuant to those requirements. **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. The Information Holder must provide notice within 30 days after the law enforcement agency determines notice will no longer impede a criminal investigation. • **Attorney general enforcement:** The attorney general can bring an action for civil penalties under the 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

Tennessee

Tenn. Code § 47-18-2107

(Scroll down to Title 47, Chapter 18, Part 21)

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

S.B. 547 (signed into law April 4, 2017)

Effective April 4, 2017

[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.

Security breach definition: Acquisition of:

(1) unencrypted computerized data; or

(2) encrypted computerized data and the encryption key

by an unauthorized person that materially compromises the security, confidentiality, or integrity of PI maintained by the Entity. "Encrypted" means computerized data that is rendered unusable, unreadable, or indecipherable without the use of a decryption process or key and in accordance with the current version of the Federal Information Processing Standard (FIPS) 140-2.

- 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 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 Entity who is discovered by the Entity to have obtained personal information and intentionally used it for an unlawful purpose.

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 if the PI was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made 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.

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:

- Social Security number;
- Driver's license number; or
- Account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	PI does not include information that is lawfully made available to the general public from federal, state, or local government records or information that has been redacted or otherwise made unusable. **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 email addresses for the 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 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; and/or • The Health Insurance Portability and Accountability Act of 1996 (HIPAA) (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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

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

H.B. 4390 (signed into law June 14, 2019)

Effective January 1, 2020

H.B. 3529 (signed into law May 26, 2021)

Effective September 1, 2021

H.B. 3746 (signed into law June 14, 2021)

Effective September 1, 2021

S.B. 768 (signed into law May 27, 2023)

Effective September 1, 2023

[BACK TO TABLE OF CONTENTS]

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

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: An Entity to which the statute applies shall disclose any breach of system security to any person, including nonresidents, whose sensitive PI was, or is reasonably believed to have been, acquired by an unauthorized person.

Attorney general notification: Any Entity that is required to provide notification of a security breach to at least 250 Texas residents, shall notify the attorney general of that breach as soon as practicable and not later than 30 days after the Entity determines that a breach has occurred. The notification must include:

- A detailed description of the nature and circumstances of the breach or the use of sensitive personal information acquired as a result of the breach;
- The number of Texas residents affected by the breach at the time of notification;
- The number of affected residents that have been sent a disclosure of the breach by mail or other direct method of communication at the time of notification;
- The measures taken by the Entity regarding the breach;
- Any measures the Entity intends to take regarding the breach after notification; and
- Information regarding whether law enforcement is investigating the breach

Businesses must submit a detailed description of the breach in addition to other required information using an electronic form accessed through the attorney general's website.

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 nationwide consumer reporting agencies 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: Notice to individuals shall be made as soon as practicable and in each case not later than the 60th day after the date on

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	which the person determines that the breach occurred, 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. • Notification to the attorney general must be made in 30 days. **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's license number or government-issued ID number; or • Account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to 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. **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 email addresses for the affected persons; • Conspicuous posting of the notice on the Entity's website; 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.

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	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. • **Attorney general website:** The attorney general will post on its publicly accessible website a listing of the notifications it receives under the statute of any system security breach. Such notices will be posted no later than 30 days after the attorney general receives the notification. The listing of the notice will be removed no later than the first anniversary of its posting if the person who provided the notification has not notified the attorney general of any additional breaches during that period. • **Attorney general 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

Utah

Utah Code §§ 13-44-101, *et seq.*

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

S.B. 193 (signed into law March 26, 2019)

Effective May 14, 2019

S.B. 127 (signed into law March 23, 2023)

Effective May 3, 2023

S.B. 98 (signed into law March 19, 2024)

Effective May 1, 2024

[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.

Attorney general notification: If an Entity must notify 500 or more UT residents, it must also notify the Office of the Attorney General, and the Utah Cyber Center. Notice shall include:

- The date the breach of system security occurred;
- The date the breach of system security was discovered;
- The total number of people affected by the breach of system security, including the total number of Utah residents affected;
- The type of personal information involved in the breach of system security; and
- A short description of the breach of system security that occurred

Notification to consumer reporting agencies: If an Entity must notify 1,000 or more UT residents, the Entity must also notify each nationwide consumer reporting agency.

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 PI 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's license number or state identification card number; or
- Account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to the person's 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	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; or • 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) **Substitute notice:** If notification in the manner described above is not feasible, 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. **Exceptions:** • **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. • **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. • **Financial institutions**: This chapter does not apply to a financial institution or affiliate of a financial institution, as defined in 15 U.S.C. § 6809. **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. The latter limitation does not apply if the violations concern more than 10,000 Utah residents and more than 10,000 residents of other states, or if the Entity agrees to settle for a greater amount. **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. • Attorney general 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	• Waiver not permitted. • Records are confidential if reported to the attorney general or Utah Cyber Center per requirements.

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

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

S. 110 (signed into law March 5, 2020)

Effective July 1, 2020

[BACK TO TABLE OF CONTENTS]

Application: Any data collector 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 a VT resident.

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 or login credentials maintained by an Entity.

- Does not include good-faith but unauthorized acquisition or access of PI or login credentials by an employee or agent of the Entity for a legitimate purpose of the Entity, provided that the PI or login credentials are 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 or login credentials is not reasonably possible and the Entity provides notice of the determination that the misuse of the PI or login credentials is not reasonably possible and a detailed explanation for said determination to the VT attorney general 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 nationwide consumer reporting agencies 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 attorney general 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 attorney general that the Entity maintains written policies and procedures to maintain the security of PI and respond 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	breaches in a manner consistent with state law shall notify the attorney general before providing notice to consumers. Notice to the attorney general shall contain the date the breach occurred, the date the breach was discovered, the number of VT residents affected, if known, and a description of the breach. If the date of the breach is unknown, then the Entity shall send notice to the attorney general or the Department as soon as the date becomes known. The Entity shall provide a copy of the notice that was provided to consumers. An Entity may also send the attorney general or Department a second copy of the notice to consumers that redacts the type of PI breached for any public disclosure of the breach. If a security breach is limited to an unauthorized acquisition of login credentials, a data collector is only required to provide notice of the security breach to the attorney general or Department of Financial Regulation, as applicable, if the login credentials were acquired directly from the data collector or its agent. **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:** Vermont's statutory requirements apply to incidents involving "personally identifiable information or login credentials." Personally identifiable information is an individual's first name or first initial and last name in combination with one or more of the following data elements, when either the name or the data elements are not encrypted, redacted or protected by another method that renders them unreadable or unusable by unauthorized persons: • Social Security number; • Driver license or nondriver State identification card number, individual taxpayer identification number, passport number, military identification card number, or other identification number that originates from a government identification document that is commonly used to verify identity for a commercial transaction; • Financial account number, credit card number, or debit card number if the number could be used without additional identifying information, access codes, or passwords; • A password, personal identification number, or other access code for a financial account; unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee of the data to identify or authenticate the consumer, such as a fingerprint, retina or iris image, 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	unique physical representation or digital representation of biometric data; • Genetic information; and • Health records or records of a wellness program or similar program of health promotion or disease prevention, a health care professional's medical diagnosis or treatment of the consumer, or a health insurance policy number PI does not mean publicly available information that is lawfully made available to the general public from federal, state, or local government records. Login credentials means a consumer's username or email address, in combination with a password or an answer to a security question, that together permit access to an online account. **Notice required:** Notice of a security breach involving PI 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 email address if (1) 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** (2) the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 (E-Sign Act) *Generally:* The notice to a consumer of a security breach involving PI 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 *Online account credentials:* If a security breach is limited to an unauthorized acquisition of login credentials for an online account other than an e-mail account, the data collector shall provide notice of the security breach to the consumer electronically or through one or more of the methods described above and shall advise the consumer to take steps necessary to protect the online account, including to change his or her login credentials for the 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	and for any other account for which the consumer uses the same login credentials. *Email account credentials:* If a security breach is limited to an unauthorized acquisition of login credentials for an email account the data collector shall not provide notice of the security breach through the email account; and the data collector shall provide notice of the security breach through one or more of the methods described above or by clear and conspicuous notice delivered to the consumer online when the consumer is connected to the online account from an IP address or online location from which the data collector knows the consumer customarily accesses the account. **Substitute notice available:** If the Entity demonstrates that the cost of providing written, email, or telephonic notice would exceed $10,000, or the Entity does not have sufficient contact information, substitute notice may be provided. Substitute notice shall consist of **all** of the following: • Conspicuously posting the notice on the Entity's website, if the Entity maintains one; and • Notifying major statewide and regional media **Exception: Compliance with other laws:** • **Interagency guidance:** 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: (1) 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 (2) 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. • **HIPAA-covered entities:** A data collector that is subject to the privacy, security, and breach notification rules adopted pursuant to the federal Health Insurance Portability and Accountability Act, is deemed to be in compliance with this subchapter if: (1) the data collector experiences a security breach that is limited to health records or records of a wellness program or similar program of health promotion or disease prevention, a health care professional's medical diagnosis or treatment of the consumer, or a health insurance policy number; and (2) the data collector provides notice to affected consumers pursuant to the requirements of the HIPAA breach notification rule. **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

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	officer's law enforcement agency engaged in 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. • Attorney general 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

Virginia

Va. Code § 18.2-186.6 (effective July 1, 2008),

§ 32.1-127.1:05 (effective January 1, 2011);

Amendment to **§ 18.2-186.6** (HB 2113) (effective July 1, 2017)

H.B. 2396 (signed into law March 18, 2019) (effective July 1, 2019)

[BACK TO TABLE OF CONTENTS]

Application: An individual, government entity, 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.

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: An Entity to which the statute applies shall disclose any 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 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, the state attorney general of the timing, distribution, and content of the notice. For health information, the Entity must also notify the Commissioner of Health.

Attorney general notification for breach of employee income tax data: Employers or payroll service providers that own or license computerized data relating to state income tax withheld must notify the attorney general of unauthorized access and acquisition of unencrypted and unredacted computerized data containing a taxpayer identification number in combination with the income tax withheld for that taxpayer that compromises the confidentiality of such data and that creates a reasonable belief that an unencrypted and unredacted version of such information was accessed and acquired by an unauthorized person, and causes, or the employer or payroll provider reasonably believes has caused or will cause, identity theft 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	fraud. For employers, the notification obligation applies only to information regarding its employees (not customers or other nonemployees). Such employer or payroll service provider shall provide the attorney general with the name and federal employer identification number of the employer without unreasonable delay after the discovery of the breach. The attorney general shall then notify the Department of Taxation of the breach. **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 the 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's license number or state identification card number issued in lieu of a driver's license number; • Account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to a resident's financial accounts; • Passport number; or • Military identification number 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;

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	• 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 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: • Email notice, if the individual or the Entity has email addresses for the members of the affected class of residents; • Conspicuous posting of the notice on the Entity's website, 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 (1) 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 (2) 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.*

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	Penalties: The state attorney general 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 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. • Attorney general 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

Washington

Wash. Rev. Code § 19.255.010 *et seq.*, § 42.56.590

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

H.B. 1071 (signed into law May 7, 2019)

Effective March 1, 2020

[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 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 to any resident of WA whose PI was, or is reasonably believed to have been, acquired by an unauthorized person and the PI 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 PI is rendered unreadable, unusable, or undecipherable by an unauthorized person).

- 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 PI 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 PI was acquired by an unauthorized person.

Attorney general notification: Any Entity that is required to issue a notification to more than 500 WA 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 following information:

- The number of WA consumers affected by the breach, or an estimate if the exact number is not known;
- A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;
- A timeframe of exposure, if known, including the date of the breach and the date of the discovery of the breach; and
- A summary of steps taken to contain the breach

The notice to the attorney general must be updated if any of the information identified above is unknown at the time the notice is due.

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 PI 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: 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 30 calendar days after the breach was discovered, unless the delay is at the request of law enforcement or the delay is due to any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	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: • Social Security number; • Driver's license number or state identification card number; • Account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account, or any other numbers or information that can be used to access a person's financial account; • Full date of birth; • Private key that is unique to an individual and that is used to authenticate or sign an electronic record; • Student, military, or passport identification number; • Health insurance policy number or health insurance identification number; • 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; or • Biometric data generated by automatic measurements of an individual's biological characteristics such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual (2) Username or email address in combination with a password or security questions and answers that would permit access to an online account; and (3) Any of the data elements or any combination of the data elements described in (1) above, without the consumer's first name or first initial and last name if the data element or combination of data elements would enable a person to commit identity theft against a consumer. PI does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. For government agencies subject to RCW 42.56.590 only, the last four digits of a social security number is included in the definition of personal information. **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) The notification must be written in plain language and must include, at a minimum, the following information:

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	• The name and contact information of the reporting person or business subject to this section; • A list of the types of PI that were or are reasonably believed to have been the subject of a breach; • A timeframe of exposure, if known, including the date of the breach and the date of the discovery of the breach; and • The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed PI **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 email addresses for the subject persons; • Conspicuous posting of the notice on the Entity's website if the Entity maintains one; and • Notification to major statewide media; or If the breach of the security of the system involves personal information including a username or password, notice may be provided electronically or by email. If the breach involves login credentials of an email account furnished by the Entity, notice may be provided using another method; not to that email address. The notice must inform the person whose personal information has been breached to promptly change his or her password and security question or answer, as applicable, or to take other appropriate steps to protect the online account with the Entity and all other online accounts for which the person uses the same username or email address and password or security question or answer. **Exception: Compliance with other laws:** • **Certain financial institutions:** 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 addition to providing notice to its primary federal regulator.

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	• **HIPAA-covered entities**: A covered entity under Health Insurance Portability and Accountability Act of 1996 (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 the aforementioned section 13402, 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. • **Attorney general enforcement:** The attorney general may bring action on behalf of the state or its residents. The violations are “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 Payment Card Industry Data Security Standard 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 Ashurst Perkins Coie’s Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

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, government entity, 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 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 nationwide consumer reporting agencies 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 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’s license number or state identification card number issued in lieu of a driver’s 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 Ashurst Perkins Coie’s Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	• Account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to 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; • A telephone number or website address that the individual may use to contact the Entity or the agent of the Entity and from whom the individual may learn what types of information the Entity maintained about that individual or about individuals in general 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: • Email notice, if the Entity has email addresses for the members of the affected class of residents; • Conspicuous posting of the notice on the Entity's website, 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 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 the Entity 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 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.

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	• **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. • Attorney general 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

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; and 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; or
- 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 nationwide consumer reporting agencies of the timing, distribution, and content of the notices sent to the individuals.

Third-party data notification: If an Entity 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

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	is not encrypted, redacted, or altered in a manner that renders the element unreadable: • Social Security number; • Driver's license number or state identification number; • Account number, 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, 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

Wyoming

Wyo. Stat. § 40-12-501 *et seq*.

(Scroll down to Title 40, Chapter 12, Article 5)

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’s license number;
- Account number, 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;
- Shared secrets or security tokens that are known to be used for database 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 Ashurst Perkins Coie’s Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	• 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; or • 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/her agent, and from which the individual may learn the toll-free contact telephone numbers and addresses for the major credit reporting agencies; • 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 • Email 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:

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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.

	• Conspicuous posting of the notice on the website of the person collecting the data, if the person maintains one; 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. • **HIPAA:** A covered entity or business associate that is subject to and complies with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), 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 HIPAA 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. • **Attorney general enforcement:** The state attorney general 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 Ashurst Perkins Coie's Privacy practice can be found at https://www.ashurstperkinscoie.com/en/insights/security-breach-notification-chart/.