HSE
Harter Secrest & Emery LLP
ATTORNEYS AND COUNSELORS
WWW.HSELAW.COM

State Data Breach Law Summary

This document is provided for informational purposes only and should not be construed as legal advice on any subject matter. You should not act or refrain from acting based on anything included in this document. Because this document contains general information, it may not reflect current legal developments or address your situation. Harter Secrest & Emery LLP disclaims all liability for actions you take or fail to take based on any content contained herein.

This State Data Breach Law Summary does not create an attorney-client relationship between you and Harter Secrest & Emery LLP. Do not rely on this document as an alternative to legal advice. You should consult a lawyer with respect to data breach issues.

If you have any questions, please contact:

F. Paul Greene
Harter Secrest & Emery LLP
1600 Bausch & Lomb Place
Rochester, NY 14604
585-231-1435
fgreene@hselaw.com

Important

This state data breach law summary is intended for informational purposes only. ***Please refer to the text of the individual state statutes for more specific information.***

Please note that this summary does not cover:

- Method of notification or substitute notification
- Contents of any required notification or required credit monitoring offerings
- Exceptions to the notification requirement with respect to good faith acquisition of personal information
- Other cybersecurity requirements in addition to data breach notification that may be included in a state data breach statute
- Implications of other applicable state or federal laws or regulations, including HIPAA and the Gramm-Leach-Bliley Act
- Exemptions for particular businesses or businesses regulated by particular industries
- Requirements or penalties for state or governmental agencies

Alabama	
Statute	Ala. Code § 8-38-1 *et seq.*
Covered Entity	A person, sole proprietorship, partnership, government entity, corporation, nonprofit, trust, estate, cooperative association, or other business entity that acquires or uses sensitive personally identifying information.
Personal Information Defined	An Alabama resident's first name or first initial and last name in combination with one or more of the following with respect to the same Alabama resident (i) A non-truncated Social Security number or tax identification number. (ii) A non-truncated driver's license number, state-issued 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. (iii) A financial account number, including a bank account number, credit card number, or debit card number, in combination with any 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. (iv) Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional. (v) An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual. (vi) A user name or email address, in combination with a password or security question and answer that would permit access to an online account affiliated with the covered entity that is reasonably likely to contain or is used to obtain sensitive personally identifying information.
What Triggers Notice Requirement	A "breach of security" or "breach" is the unauthorized acquisition of data in electronic form containing sensitive personally identifying information. Acquisition occurring over a period of time committed by the same entity constitutes one breach. If an entity determines that sensitive personally identifying information has been acquired or is reasonably believed to have been acquired by an unauthorized person, and is reasonably likely to cause substantial harm to the individuals to whom the information relates, the covered entity shall give notice to each individual. If a covered entity determines that a breach of security has or may have occurred in relation to sensitive personally identifying information that is accessed, acquired, maintained, stored, utilized, or

Alabama

	communicated by, or on behalf of, the covered entity, the covered entity shall conduct a good faith and prompt investigation that includes all of the following: (i) An assessment of the nature and scope of the breach. (ii) Identification of any sensitive personally identifying information that may have been involved in the breach and the identity of any individuals to whom that information relates. (iii) A determination of whether the sensitive personally identifying information has been acquired or is reasonably believed to have been acquired by an unauthorized person, and is reasonably likely to cause substantial harm to the individuals to whom the information relates. (iv) Identification and implementation of measures to restore the security and confidentiality of the systems compromised in the breach. In determining whether sensitive personally identifying information has been acquired or is reasonably believed to have been acquired by an unauthorized person without valid authorization, the following factors may be considered: (i) 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. (ii) Indications that the information has been downloaded or copied. (iii) Indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported. (iv) Whether the information has been made public. If notification is not required, the entity must document that decision in writing and maintain it for no less than 5 years.
Encryption/Redaction Safe Harbor	Notification is not required if the information compromised is truncated, 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, including encryption of the data, document, or device containing the sensitive personally identifying information, unless the covered entity knows or has reason to know that the encryption key or security credential that could render the personally identifying information readable or useable has been breached together with the information.
Exemptions from Notification	Notification is not required if the entity determines that the breach is not reasonably likely to cause substantial harm to the individuals to whom the information relates.

Alabama

Timing of Notification	Notice to individuals shall be made as expeditiously as possible and without unreasonable delay, taking into account the time necessary to allow the covered entity to conduct an investigation, as described above. Notification may be delayed if a law enforcement agency determines that notice would interfere with a criminal investigation or national security and makes a written request for the delay. If the number of people to be notified exceeds 1000, the entity shall provide written notice to the attorney general as expeditiously as possible and without unreasonable delay. If the number of people to be notified exceeds 1000, the entity shall provide notice to all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis without unreasonable delay.
Penalties/Private Cause of Action	A violation of the notification provisions of this chapter is an unlawful trade practice, but does not constitute a criminal offense. The attorney general shall have the exclusive authority to bring an action for civil penalties under this chapter. A violation of this chapter does not establish a private cause of action for a deceptive trade practice. Any covered entity or third-party agent who is knowingly engaging in or has knowingly engaged in a violation of the notification provisions of this chapter is subject to the penalty provisions set out for deceptive trade practices. Civil penalties assessed for a deceptive trade practice violation shall not exceed five hundred thousand dollars ($500,000) per breach. A covered entity that violates the notification provisions of this chapter shall be liable for a civil penalty of not more than five thousand dollars ($5,000) per day for each consecutive day that the covered entity fails to take reasonable action to comply with the notice provisions of this chapter. The attorney general shall have the exclusive authority to bring an action for damages in a representative capacity on behalf of any named individual or individuals. In such an action brought by the office of the Attorney General, recovery shall be limited to actual damages suffered by the person or persons, plus reasonable attorney's fees and costs

Alaska	
Statute	Alaska Stat. § 45.48.010 *et seq.*
Covered Entity	An information collector is a person doing business, a government agency, or a person with more than 10 employees, who owns or licenses personal information of a state resident in any form.
Personal Information Defined	An individual's (i) first name or first initial and (ii) last name, plus one or more of the following elements: (i) social security number; (ii) driver's license number or state identification card number; (iii) individual's account number, credit card number, or debit card number, but if the account or card can only be accessed by a personal code (security code, access code, personal identification number or password), then the account number, credit card number, or debit card number with the personal code; and (iv) passwords, personal identification numbers, or other access codes for financial accounts.
What Triggers Notice Requirement	"Breach of security" means unauthorized acquisition, or reasonable belief of unauthorized acquisition, of personal information that compromises the security, confidentiality, or integrity of the personal information maintained by the information collector. "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 another method. The entity must disclose a breach of security to the affected Alaska residents, after discovery or notification of the breach.
Encryption/Redaction Safe Harbor	Notification is not required if the information was encrypted or redacted, unless the encryption key was also accessed or acquired.
Exemptions from Notification	Notice is not required if, after an appropriate investigation and written notice to the attorney general, the entity determines there is not a reasonable likelihood that harm to the consumers has or will result from the breach. This determination must be documented in writing and maintained for five years.
Timing of Notification	Notification to affected state residents must be provided in the most expeditious time possible and without unreasonable delay, as necessary to determine the scope of the breach and restore the reasonable integrity of the information system.

Alaska	
	Notification may be delayed if an appropriate law enforcement agency determines that disclosing the breach will interfere with a criminal investigation. Notification must be made after law enforcement informs the information collector in writing that notification will no longer interfere with the investigation. If more than 1000 state residents are notified, notification to consumer credit reporting agencies that compile and maintain files on consumers on a nationwide basis must be made without unreasonable delay.
Penalties/Private Cause of Action	If an information collector that is not a governmental agency violates the statute, the violation is an unfair or deceptive act or practice under state law. The information collector is liable to the state for a civil penalty of up to $500 for each state resident who was not notified, except that the total civil penalty may not exceed $50,000. Damages may also be awarded under AS 45.50.531 (private and class actions) but are limited to actual economic damages that do not exceed $500. Attorney's fees, costs under AS 45.50.537 and damages are limited to actual economic damages.

Arizona	
Statute	Ariz. Rev. Stat. § 18-551 *et seq.*
Covered Entity	A natural person, corporation, business trust, estate, trust, partnership, association, joint venture, government or government subdivision or agency or any other legal or commercial entity, that conducts business in Arizona and that owns, maintains or licenses unencrypted and unredacted computerized personal information.
Personal Information Defined	An individual's first name or first initial and last name in combination with one or more specified data elements: (i) social security number; (ii) driver's license or nonoperating identification license; (iii) private key that is unique to an individual and that is used to authenticate or sign an electronic record; (iv) financial account number or credit or debit card number in combination with any required security code, access code or password that would allow access to the individual's financial account; (v) health insurance identification number; (vi) medical or mental health treatment or diagnosis by a health care professional; (vii) passport number; (viii) taxpayer identification number or an identity protection personal identification number issued by the IRS; and (ix) unique biometric data generated from a measurement or analysis of human body characteristics to authenticate an individual when the individual accesses an online account. Also, an individual's user name or e-mail address, in combination with a password or security question and answer, that allows access to an online account.
What Triggers Notice Requirement	"Breach" means an unauthorized acquisition of and unauthorized access that materially compromises the security or confidentiality of unencrypted and unredacted computerized personal information maintained as part of a database of personal information regarding multiple residents of Arizona, who have principal mailing addresses in Arizona as reflected in the records of the person conducting business in Arizona at the time of the breach. "Security Incident" means an event that creates reasonable suspicion that a person's information systems or computerized data may have been compromised or that measures put in place to protect the person's information systems or computerized data may have failed.

Arizona	
	When a person becomes aware of a security incident, it must conduct an investigation to promptly determine whether there has been a security system breach. If a determination is made that there has been a security system breach, the person who owns or licenses the computerized data must notify the state residents affected.
Encryption/Redaction Safe Harbor	Notification is not required if the accessed personal information was encrypted or redacted.
Exemptions from Notification	Notification is not required if the person, an independent third-party forensic auditor or a law enforcement agency determines after a reasonable investigation that a security system breach has not resulted or is not reasonably likely to result in substantial economic loss to affected individuals.
Timing of Notification	Notification must be made within 45 days of the determination that a security system breach has occurred. Notice may be delayed if a law enforcement agency advises the person that the notification will impede a criminal investigation. Once the law enforcement agency informs the personal that notifications no longer compromise the investigation, the person must make the required notifications within 45 days. If notification to more than 1000 state residents is required, the person must also notify the three largest nationwide consumer reporting agencies, and the attorney general.
Penalties/Private Cause of Action	A knowing and willful violation of this statute is considered an unlawful practice pursuant to A.R.S. 44-1522. Only the attorney general may enforce such a violation. A civil penalty imposed for a violation of this statute will not exceed the lesser of $10,000 per affected individual or the total amount of economic loss sustained by affected individuals. The maximum civil penalty from a breach or series of related breaches may not exceed $500,000. The attorney general may also recover restitution for affected individuals.

Arkansas	
Statute	Ark. Code § 4-110-101 *et seq.*
Covered Entity	A business is a sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the law of this state, any other state, the United States, or of any other country or the parent or the subsidiary of a financial institution.
Personal Information Defined	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: (i) social security number; (ii) driver's license or Arkansas identification card number; (iii) 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; (iv) medical information; or (v) biometric data, defined as data generated by automatic measurements of an individual's biological characteristics, including, without limitation: fingerprints, faceprint, retinal or iris scan, hand geometry, voiceprint analysis, DNA, or any other unique biological characteristics of an individual if the characteristics are used by the owner or licensee to uniquely authenticate the individual's identity when the individual accesses a system or account.
What Triggers Notice Requirement	"Breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person or business. Any person or business that acquires, owns or licenses computerized data that includes personal information must disclose any breach of the security system following discovery or notification of the breach to any affected Arkansas residents, after discovery or notification of the breach, if unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. A written determination of a breach and supporting documentation must be kept for five years from the date of determination of the breach.
Encryption/Redaction Safe Harbor	Notification is not required if the accessed personal information was encrypted or redacted.

Arkansas	
Exemptions from Notification	No notice is required if, after a reasonable investigation, the person or business determines there is no reasonable likelihood of harm to customers.
Timing of Notification	Notification must be given in the most expedient manner 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 data system. Notification may be if a law enforcement agency determines that the notification will impede a criminal investigation. Notification shall be made after the law enforcement agency determines it will not compromise the investigation. If a breach affects the personal information of more than 1000 individuals, the person or business must also, at the same time notification is given to individuals or within 45 days after the person or business determines there is a reasonable likelihood of harm to customers, whichever occurs first, disclose the breach to the attorney general.
Penalties/Private Cause of Action	Any violation of this statute is punishable by action of the attorney general, who may bring an action under A.R.S. 4-8-101 *et seq.* (a deceptive trade practice).

California	
Statute	Cal. Civ. Code § 1798.80 *et seq.*; Cal. Health & Safety Code § 1280.15
Covered Entity	**General Breach Notification Statute**: Businesses that conduct business in this state, and that own or license computerized data that includes personal information. A business is a sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the law of this state, any other state, the United States, or of any other country, or the parent or the subsidiary of a financial institution. A business also includes an entity that disposes of records. **Medical Information Breach Notification Statute**: A clinic, health facility, home health agency, or hospice.
Personal Information Defined	**General Breach Notification Statute**: 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 not encrypted or redacted: (i) social security number; (ii) driver's license number, California 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; (iii) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (iv) medical information; (v) health insurance information; (vi) unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual; and (vii) information or data collected through the use or operation or an automated license plate recognition system. Also, a username or email address in combination with a password or security question and answer that would permit access to an online account. **Medical Information Breach Notification Statute**: Patients' medical information. "Medical information" is any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or

California

	contractor regarding a patient's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional. "Individually identifiable" means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the individual's identity.
What Triggers Notice Requirement	**General Breach Notification Statute**: A breach of the security of the system is the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. The business must disclose a breach of the security of the system, following discovery or notification of the breach, to a California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person, or whose encrypted personal information 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 business has a reasonable belief that the encryption key or security credential could render that personal information readable or useable. **Medical Information Breach Notification Statute**: The statute is triggered by any unlawful or unauthorized access to, or use or disclosure of a patient's medical information. "Unauthorized" means the inappropriate access, review, or viewing of patient medical information without a direct need for medical diagnosis, treatment, or other lawful use as permitted by the Confidentiality of Medical Information Act or any other statute or regulation governing the lawful access, use, or disclosure of medical information.
Encryption/Redaction Safe Harbor	**General Breach Notification Statute**: Notification is not required if the accessed personal information was encrypted.
Exemptions from Notification	N/A
Timing of Notification	**General Breach Notification Statute**: Disclosure must be made in the most expedient time possible, and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. Notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification must be made promptly after the law enforcement agency determines that it will not compromise the investigation.

California	
	If more than 500 state residents are notified, the business must electronically submit a single sample copy of the notification, excluding any personally identifiable information, to the attorney general. **Medical Information Breach Notification Statute**: Affected patients and the California Department of Health Services must be notified no later than **15 business days** after the unauthorized access, use, or disclosure has been detected. This notice can be delayed for law enforcement purposes if the delay is requested by the law enforcement agency and specifies a date on which the delay shall end. The delay must be documented by the covered entity.
Penalties/Private Cause of Action	**General Breach Notification Statute**: Any customer injured by a violation of this statute may institute a civil action to recover damages. Any business that violates or proposes to violate this statute may be enjoined. **Medical Information Breach Notification Statute**: The California Department of Health Services may impose the following penalties against entities that violate the statute: (1) $25,000 per patient whose information was unlawfully or without authorization accessed, used or disclosed, and up to $17,500 per subsequent occurrence; (2) entities that fail to report the incident to the State Department of Health Services or the affected patients within the 15 day time period absent lawful delay are subject to a penalty of $100 per day; and (3) the total penalties imposed may not exceed $250,000 per reported event.

Colorado	
Statute	Colo. Rev. Stat. § 6-1-716
Covered Entity	An individual, corporation, business trust, estate, trust, partnership, unincorporated association, or two or more thereof having a joint or common interest, or any other legal or commercial entity, that maintains, owns, or licenses personal information in the course of the entity's business, vocation, or occupation.
Personal Information Defined	A Colorado 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: (i) Social security number; (ii) student, military, or passport identification number; (iii) driver's license number or identification card number; (iv) medical information; (v) health insurance identification number; or (vi) biometric data. A Colorado resident's username or e-mail address, in combination with a password or security questions and answers, that would permit access to an online account. A Colorado resident's account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to that account.
What Triggers Notice Requirement	"Security Breach" means the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained, owned or licensed by a covered entity. The entity must, when it becomes aware of a breach of the security of the system, conduct in good faith a prompt investigation to determine the likelihood that personal information has been or will be misused. The entity must give notice to the affected Colorado resident unless the investigation determines that the misuse of information has not occurred and is not reasonably likely to occur.
Encryption/Redaction Safe Harbor	Notification is not required if the accessed personal information was encrypted, redacted or secured by any other method rendering the name or element unreadable or unusable and the confidential process, encryption key, or other means to decipher the secured information was also acquired in the security breach or reasonably believed to have been acquired.
Exemptions from Notification	Notification is not required if after a good faith, prompt investigation, the entity determines that misuse of personal information about a

Colorado	
	Colorado resident has not occurred and is not reasonably likely to occur.
Timing of Notification	Notification is to be made as expediently as possible, and without unreasonable delay, but not later than 30 days after the date of determination that a security breach occurred, unless law enforcement determines that notice will impede a criminal investigation. Delay is also permitted to determine the nature and scope of the breach and to restore the reasonable integrity of the computerized data system. If 500 or more Colorado residents were affected, the covered entity must also notify the attorney general in the most expedient time possible and without unreasonable delay, but not more than 30 days after the date of determination that a security breach occurred. If more than 1000 Colorado residents are notified, the covered entity shall also notify, in the most expedient time possible and without unreasonable delay, all consumer reporting agencies that compile and maintain files on a nationwide basis.
Penalties/Private Cause of Action	The Attorney General may bring an action in law or equity to address violations of this statute and for other relief that may be appropriate to ensure compliance with this statute or to recover direct economic damages resulting from a violation, or both.

Connecticut	
Statute	Conn. Gen. Stat. § 36a-701b
Covered Entity	Any person who conducts business in this state, and who, in the ordinary course of such person's business, owns, licenses or maintains computerized data that includes personal information.
Personal Information Defined	An individual's first name or first initial and last name in combination with any one, or more, of the following data: (i) Social Security number; (ii) driver's license number or state identification card number; (iii) credit or debit card number; or (iv) financial account number in combination with any required security code, access code or password that would permit access to such financial account.
What Triggers Notice Requirement	"Breach of security" means unauthorized access to or unauthorized acquisition of electronic files, media, databases, or computerized data containing personal information not secured by encryption or another method that renders the personal information unreadable or unusable. An entity must give notice of any breach of security after it is discovered to any Connecticut resident whose personal information was or is reasonably believed to have been breached.
Encryption/Redaction Safe Harbor	Notification is not required if the accessed personal information was encrypted or otherwise unreadable or unusable.
Exemptions from Notification	Notification is not required if, after appropriate investigation and consultation with law enforcement, the entity reasonably determines that the breach will not likely result in harm to the affected individuals.
Timing of Notification	Disclosure must be made without unreasonable delay, but not later than 90 days after discovery of the breach (unless a shorter time is required under an applicable federal law), subject to delay at the request of law enforcement agencies if it will impede a criminal investigation and/or to complete an investigation to determine the nature and scope of the breach, to identity the individuals affected, or to restore the reasonable integrity of the data system. If notice is delayed at the request of law enforcement, it may only be given after approval by the applicable law enforcement agency. If notice to individuals is required, then notice is also required to the attorney general not later than the time when the notice is provided to the affected individuals.
Penalties/Private Cause of Action	Failure to comply with this statute constitutes an unfair trade practice under Conn. Gen. Stat. § 42-110b and is enforced by the attorney general.

Delaware	
Statute	6 Del. Code § 12B-101 *et seq.*
Covered Entity	An individual, corporation, business trust, estate trust, partnership, limited liability company, association, joint venture, government, governmental subdivision, agency, or instrumentality, public corporation, or any other legal or commercial entity, that conducts business in this State and that owns or licenses computerized data that includes personal information.
Personal Information Defined	A Delaware resident's first name or first initial and last name in combination with any 1 or more of the following data elements that relate to that individual: (i) Social Security number. (ii) Driver's license number or state or federal identification card number. (iii) 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. (iv) Passport number. (v) A username or email address, in combination with a password or security question and answer that would permit access to an online account. (vi) Medical history, medical treatment by a health-care professional, diagnosis of mental or physical condition by a health care professional, or deoxyribonucleic acid profile. (vii) Health insurance policy number, subscriber identification number, or any other unique identifier used by a health insurer to identify the person. (viii) Unique biometric data generated from measurements or analysis of human body characteristics for authentication purposes. (ix) An individual taxpayer identification number.
What Triggers Notice Requirement	"Breach of security" means the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information. An entity must give notice following a determination of a breach of security to any resident whose personal information was breached or is reasonably believed to have been breached, unless, after an appropriate investigation, the person reasonably determines that the breach of security is unlikely to result in harm to the individuals whose personal information has been breached.

Delaware	
Encryption/Redaction Safe Harbor	Notification is not required if the accessed personal information was encrypted unless the unauthorized acquisition includes, or is reasonably believed to include, the encryption key and the entity that owns or licenses the encrypted information has a reasonable belief that the encryption key could render that personal information readable, useable or decipherable.
Exemptions from Notification	Notification is not required if, after an appropriate investigation, the entity reasonably determines that the breach of security is unlikely to result in harm to the individuals whose personal information has been breached.
Timing of Notification	Disclosure must be made in the most expedient time possible and without unreasonable delay, but not later than 60 days after determination of the breach of security, except if (1) a shorter time is required by federal law; (2) a law enforcement agency determines notice will impede a criminal investigation; or (3) when an entity otherwise required to provide notice could not, through reasonable diligence, identify within 60 days that the personal information of certain residents of this State was included in a breach of security, such person must provide notice to such residents as soon as practicable after the determination that the breach of security included the personal information of such residents, unless such person provides or has provided substitute notice. If the number of affected residents exceeds 500 residents, the attorney general must also receive notice not later than the time notice is provided to the resident.
Penalties/Private Cause of Action	The Attorney General may bring an action in law or equity to address violations of this chapter and for other relief that may be appropriate to ensure proper compliance with this chapter or to recover direct economic damages resulting from a violation, or both.

District of Columbia	
Statute	D.C. Code § 28-3851 *et seq.*
Covered Entity	Any person or entity who conducts business in the District of Columbia, and who, in the course of such business, owns or licenses computerized or other electronic data that includes personal information.
Personal Information Defined	A person's first name or first initial and last name, or phone number, or address, in combination with one or more of the following: (i) 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; (ii) Account number, credit card 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; (iii) Medical information;. (iv) Genetic information and deoxyribonucleic acid profile; (v) 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; (vi) 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 (vii) Any combination of the above data 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. Or any other number or code or combination of numbers or codes, such as account number, security code, access code, or password, that allows access to or use of an individual's financial or credit account.
What Triggers Notice Requirement	"Breach of the security of the system" means unauthorized acquisition of computerized or other electronic data, or any equipment or device storing such data that compromises the security, confidentiality, or integrity of personal information. When an entity discovers a breach

District of Columbia	
	of the security of the system it shall promptly notify any District of Columbia resident whose personal information was included in the breach.
Encryption/Redaction Safe Harbor	Notification is not required if the accessed personal information was secure and thus unusable by an unauthorized third party.
Exemptions from Notification	N/A
Timing of Notification	Notification shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, if law enforcement determines that notification will impede a criminal investigation, and any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. If an entity is required to notify more than 50 people of a breach, the entity shall also notify the attorney general no later than such notice is provided to individuals. If an entity is required to notify more than 1000 people of a breach, the entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.
Penalties/Private Cause of Action	Any District of Columbia resident injured by a violation of this statute or by an entities' failure to maintain "reasonable security safeguards" may institute a civil action to recover actual damages, the costs of the action, and reasonable attorney's fees. Actual damages do not include dignitary damages, including pain and suffering. The attorney general may petition the Superior Court for the District of Columbia for temporary or permanent injunctive relief and for an award of restitution for property lost or damages suffered by District of Columbia residents due to a violation of this statute. The attorney general may recover a civil penalty not to exceed $100 for each violation, the costs of the action, and reasonable attorney's fees. Each failure to notify a District of Columbia resident constitutes a separate violation.

Florida	
Statute	Fla. Stat. § 501.171
Covered Entity	A sole proprietorship, partnership, corporation, trust, estate, cooperative, association, governmental entity, or other commercial entity that acquires, maintains, stores, or uses personal information.
Personal Information Defined	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: (i) A social security number; (ii) A driver license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity; (iii) A financial account number or credit or debit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual's financial account; (iv) Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or (v) An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual. A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account.
What Triggers Notice Requirement	"Breach" or "breach of security" means unauthorized access of data in electronic form containing personal information. The entity must give notice to each Florida resident whose personal information was, or is reasonably believed to have been, accessed because of a breach.
Encryption/Redaction Safe Harbor	Notification is not required if the accessed personal information was encrypted, secured or modified by any other method or technology that removes personally identifying information or renders the information unusable.
Exemptions from Notification	Notification is not required if, after an investigation and consultation with law enforcement, 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 personal information was accessed. This determination must be in writing and maintained for at least 5 years. The entity must give this writing to the Florida Department of Legal Affairs within 30 days after the determination.

Florida	
Timing of Notification	Notice must be made as expeditiously as practicable and without unreasonable delay, taking into account the time necessary to allow the entity to determine the scope of the breach, to identify affected individuals, and to restore the reasonable integrity of the data system, but no later than 30 days after the determination of a breach or reason to believe a breach occurred. An entity may receive 15 additional days to provide notice to individuals if good cause for delay in provided in writing to the Department within 30 days after determination of the breach or reason to believe the breach occurred. Notification may be delayed if law enforcement determines that notice would interfere with a criminal investigation and makes a written request to delay the notice to a specified date. If 500 or more individuals in the state are affected, the entity must provide notice to the Department of Labor Affairs as expeditiously as practicable, but not later than 30 days after the determination of the breach or reason to believe a breach occurred. If notice of more than 1000 individuals is required, the entity must also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.
Penalties/Private Cause of Action	A violation of this section shall be treated as an unfair or deceptive trade practice in any action brought by the Department of Labor Affairs. A entity is liable for a civil penalty not to exceed $500,000. There is no private right of action.

Georgia	
Statute	Ga. Code § 10-1-910 *et seq.*
Covered Entity	Data Collectors, including any state or local agency or subdivision thereof including any department, bureau, authority, public university or college, academy, commission, or other government entity; provided, however, that the term "data collector" shall not include 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. Information brokers, including any individual, partnership, corporation, limited liability company, trust, estate, cooperative, association, or other that, for monetary fees or dues, engages in whole or in part in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring, or communicating information concerning individuals for the primary purpose of furnishing personal information to nonaffiliated third parties, but does not include any governmental agency whose records are maintained primarily for traffic safety, law enforcement, or licensing purposes.
Personal Information Defined	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: (i) Social security number; (ii) Driver's license number or state identification card number; (iii) 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; (iv) Account passwords or personal identification numbers or other access codes; or (v) Any of the above items (i) through (iv) 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.
What Triggers Notice Requirement	"Breach of the security of the system" means unauthorized acquisition of an individual's electronic data that compromises the security, confidentiality, or integrity of personal information. Any covered entity that maintains computerized data including personal information must give notice of any breach of the security of the system following discovery or notification of the breach to any resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Georgia	
Encryption/Redaction Safe Harbor	Notification is not required if the accessed personal information was encrypted or redacted.
Exemptions from Notification	N/A
Timing of Notification	Notice shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement in determining whether a criminal investigation will be compromised or with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system. If more than 10,000 residents of this state are notified, the entity must also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.
Penalties/Private Cause of Action	N/A

Hawaii	
Statute	Haw. Rev. Stat. § 487N-1 *et seq.*
Covered Entity	Any business that owns or licenses personal information of residents of Hawaii, any business that conducts business in Hawaii that owns or licenses personal information in any form (whether computerized, paper, or otherwise), or any government agency that collects personal information for specific government purposes. A business is any sole proprietorship, partnership, corporation, association, or other group, however organized, and whether or not organized to operate at a profit. The term includes a financial institution organized, chartered, or holding a license or authorization certificate under the laws of the State, any other state, the United States, or any other country, or the parent or the subsidiary of any such financial institution
Personal Information Defined	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: (i) Social Security number; (ii) Driver's license number or Hawaii identification card number; or (iii) Account number, credit or debit card number, access code, or password that would permit access to an individual's financial account.
What Triggers Notice Requirement	"Security breach" means an incident of unauthorized access to and acquisition of unencrypted or unredacted records or data containing personal information where illegal use of the personal information has occurred or is reasonably likely to occur and that creates a risk of harm to a person. The affected person must be notified that there has been a security breach after discovery or notification of the breach.
Encryption/Redaction Safe Harbor	Notification is not required if the accessed personal information was encrypted or redacted, unless the confidential process or key was also accessed.
Exemptions from Notification	N/A
Timing of Notification	Notification shall be made without unreasonable delay, consistent with the legitimate needs of law enforcement and 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. Law enforcement may delay notification based upon a determination that notification may impede a criminal investigation or jeopardize national security if it requests the delay in writing or the request is documented by the entity in writing.

Hawaii	
	If a business provides notice to more than 1000 people at one time, the business shall notify in writing, without unreasonable delay, the State of Hawaii's office of consumer protection and all consumer reporting agencies that compile and maintain files on a nationwide basis.
Penalties/Private Cause of Action	Any business that violates this statute shall be subject to penalties of not more than $2,500 for each violation. The attorney general or the executive director of the Office of Consumer Protection may bring an action pursuant to this section. Any business that violates this statute shall be liable to the injured party in an amount equal to the sum of any actual damages sustained by the injured party because of the violation. The court in any action brought under this section may award reasonable attorney's fees to the prevailing party.

Idaho	
Statute	Idaho Code § 28-51-104 *et seq.*
Covered Entity	Individuals and commercial entities, which include corporations, business trusts, estates, trusts, partnerships, limited partnerships, limited liability partnerships, limited liability companies, associations, organizations, joint ventures and any other legal entities, whether for profit or not-for-profit, that conduct business in Idaho and that own or license computerized data that includes personal information about a resident of Idaho.
Personal Information Defined	An Idaho resident's first name or first initial and last name in combination with any one (1) or more of the following data elements that relate to the resident, when either the name or the data elements are not encrypted: (i) Social security number; (ii) Driver's license number or Idaho identification card number; or (iii) Account number, or credit 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.
What Triggers Notice Requirement	"Breach of the security of the system" means the illegal acquisition of unencrypted computerized data that materially compromises the security, confidentiality, or integrity of personal information for one or more persons. The entity shall, when it becomes aware of a breach, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has or will be misused. If the investigation determines that the misuse of personal information has occurred or is reasonably likely to occur, the entity must give notice as soon as possible to the affected Idaho resident.
Encryption/Redaction Safe Harbor	Notification is not required if the accessed personal information was encrypted.
Exemptions from Notification	Notification is not required if an investigation determines that the misuse of information about an Idaho resident has not occurred and is not reasonably likely to occur.
Timing of Notification	Notice must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and any measures necessary to determine the scope of the breach, identify the individuals affected, and to restore the reasonable integrity of the computerized data system. Notice may be delayed if a law enforcement agency advises the entity that the notice will impede a criminal investigation.
Penalties/Private Cause of Action	Any entity that intentionally fails to give notice shall be subject to a fine of not more than $25,000 per breach of the security of the system.

Idaho	
	The entity may also be subject to a civil action by its primary regular to enjoin it from further violations.

Illinois	
Statute	815 Ill. Comp Stat. 530/1 *et seq.*
Covered Entity	Government agencies, public and private universities, privately and publicly held corporations, financial institutions, retail operators, and any other entity that, for any purpose, handles, collects, disseminates, or otherwise deals with nonpublic personal information, that own or license personal information concerning an Illinois resident.
Personal Information Defined	An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the name or data elements have been acquired without authorization through the breach of security: (i) Social Security number. (ii) Driver's license number or State identification card number. (iii) Account number or credit 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. (iv) Medical information or, 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. (v) Health insurance information 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 medical information in an individual's health insurance application and claims history, including any appeals records. (vi) 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. User name or email address, in combination with a password or security question and answer that would permit access to an online account, when either the user name or email address or password or security question and answer are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the data elements have been obtained through the breach of security.
What Triggers Notice Requirement	"Breach" or "breach of the security of the system data" means the unauthorized acquisition of computerized data that compromises the

Illinois	
	security, confidentiality, or integrity of personal information. After an entity discovers or is notified of a breach, it must notify the affected Illinois resident.
Encryption/Redaction Safe Harbor	Notification is not required if the accessed personal information was encrypted or redacted.
Exemptions from Notification	N/A
Timing of Notification	Notification 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, security, and confidentiality of the data system. Notification may be delayed if law enforcement determines that notification will interfere with a criminal investigation and provides a written request to the entity for the delay. If notification is required to be sent to more than 500 Illinois residents, the covered entity shall provide notice to the Attorney General of the breach. Such notice must be made in the most expedient time possible and without unreasonable delay, but in no event later than when notice is provided to Illinois residents. If the date of the breach is unknown when notice is sent to the Attorney General, the date of the breach shall be sent to the Attorney General as soon as possible.
Penalties/Private Cause of Action	Violations constitute an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act.

Indiana	
Statute	Ind. Code §§ 24-4.9-1-1 *et seq.*
Covered Entity	An individual, a corporation, a business trust, an estate, a trust, a partnership, an association, a nonprofit corporation or organization, a cooperative, or any other legal entity, that owns or licenses computerized data that includes personal information.
Personal Information Defined	A Social Security number that is not encrypted or redacted; or an individual's first and last names, or first initial and last name, and one (1) or more of the following data elements that are not encrypted or redacted: (i) A driver's license number. (ii) A state identification card number. (iii) A credit card number. (iv) 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.
What Triggers Notice Requirement	"Breach of the security of data" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information. The term includes the unauthorized acquisition of computerized data that have been transferred to another medium, including paper, microfilm, or a similar medium, even if the transferred data are no longer in a computerized format. After the entity discovers or is notified of a breach, and the entity knows, should know, or should have known, that the unauthorized acquisition constituting the breach has resulted in or could result in identity deception, identity theft, or fraud, it must disclose the breach to Indiana residents.
Encryption/Redaction Safe Harbor	Notification is not required if the accessed personal information was redacted or encrypted, unless the unauthorized recipient acquired or had access to the encryption key, or the key was compromised or disclosed.
Exemptions from Notification	Notification is not required if the entity unauthorized acquisition constituting the breach has not resulted in or could not result in identity deception, identity theft, or fraud.
Timing of Notification	Notification must be made without unreasonable delay. A delay is reasonable if it is: (i) necessary to restore the integrity of the computer system; (ii) necessary to discover the scope of the breach; or (iii) in response to a request from the Indiana Attorney General or a law enforcement agency to delay disclosure because disclosure will: a. impede a criminal or civil investigation; or b. jeopardize national security.

Indiana	
	Notification must be made as soon as possible after the delay is no longer necessary to restore the integrity of the computer system or to discover the scope of the breach, or the attorney general or law enforcement agency notifies the person that the delay will no longer impede a criminal or civil investigation or jeopardize national security. Notification is also required to the attorney general. If more than 1000 consumers must notified, then the entity shall also notify to each consumer reporting agency that compiles and maintains files on consumers on a nationwide basis.
Penalties/Private Cause of Action	A person that is required to make a disclosure or notification in accordance with this statute and that fails to comply with any provision of this article commits a deceptive act that is actionable only by the attorney general. A deceptive act is the failure to make a required disclosure or notification in connection with a related series of breaches. The attorney general may bring an action for: (i) An injunction to enjoin future violations; (ii) A civil penalty of not more than $150,000 per deceptive act; (iii) The attorney general's reasonable costs in the investigation and maintaining the action.

Iowa	
Statute	Ia. Code §§ 715C.1 *et. seq.*
Covered Entity	Any individual; corporation; business trust; estate; trust; partnership; limited liability company; association; joint venture; government; governmental subdivision, agency, or instrumentality; public corporation; or any other legal or commercial entity, that owns or licenses computerized data that includes a consumer's personal information that is used in the course of the person's business, vocation, occupation, or volunteer activities.
Personal Information Defined	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, unredact, or otherwise read the data elements have been obtained through the breach of security: (i) Social security number. (ii) Driver's license number or other unique identification number created or collected by a government body. (iii) Financial account number, 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. (iv) 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. (v) Unique biometric data, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data.
What Triggers Notice Requirement	"Breach of security" means unauthorized acquisition of personal information maintained in computerized form by a person that compromises the security, confidentiality, or integrity of the personal information. It also means unauthorized acquisition of personal information maintained in any medium, including on paper, that was transferred to that medium from computerized form and that compromises the security, confidentiality, or integrity of the personal information. An entity that was subject to a breach of security must give notice of the breach of security after discovery of the breach or receipt of notification to any consumer whose personal information was included in the breached information.
Encryption/Redaction Safe Harbor	Notification is not required if the accessed personal information was encrypted, redacted, or otherwise altered in a way that makes the name or data elements unreadable, unless the keys to unencrypt,

Iowa	
	unredact, or otherwise read the data were obtained through the security breach.
Exemptions from Notification	Notification is not required if, after an appropriate investigation or after consultation with federal, state, or local law enforcement agencies it is determined that there is no reasonable likelihood of financial harm to the consumers whose personal information was acquired. This determination must be documented in writing and kept for five years.
Timing of Notification	Notification must be made in the most expeditious manner possible and without unreasonable delay consistent with the legitimate needs of law enforcement and any measures necessary to sufficiently determine contact information of the consumers, determine the scope of the breach, and restore the reasonable integrity, security, and confidentiality of the data. Notice requirements may be delayed if a law enforcement agency determines that notification will impede a criminal investigation and the agency makes a written request that notification be delayed. If notification to more than 500 residents of Indiana, written notice must also be made to the consumer protection division of the office of the attorney general within five days after giving notice of the breach to any consumer.
Penalties/Private Cause of Action	Violations are an unlawful practice under Iowa's Consumer Fraud Statute. The attorney general may also seek and obtain an order that a party held to violate this section pay damages to the attorney general on behalf of a person injured by the violation.

Kansas	
Statute	Kan. Stat. §§ 50-7a01 *et seq.*
Covered Entity	Any individual, partnership, corporation, trust, estate, cooperative, association, government, or governmental subdivision or agency or other entity that conducts business in this state and that owns or licenses computerized data that includes personal information.
Personal Information Defined	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: (i) Social security number; (ii) driver's license number or state identification card number; or (iii) financial account number, or credit 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. The term "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state or local government records.
What Triggers Notice Requirement	"Security breach" means the unauthorized access and acquisition of unencrypted or unredacted computerized data that compromises the security, confidentiality or integrity of personal information and that causes or is reasonably believed has or will cause identity theft to any consumer. When the entity becomes aware of any security breach it must conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused. If the investigation determines that the misuse of personal information has occurred or is reasonably likely to occur, the entity must notify the affected Kansas resident as soon as possible.
Encryption/Redaction Safe Harbor	Notification is not required if the accessed personal information was encrypted or redacted.
Exemptions from Notification	Notification is not required if the entity determines that the incident did not cause, or the entity does not reasonably believe will cause, identity theft to the consumer. Notification is also not required if the investigation concludes that personal information has or will be misused.
Timing of Notification	Notification of a breach must be provided in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system. Notice can be delayed if a law enforcement agency determines that notice will impede a criminal investigation.

Kansas	
	If more than 1000 consumers require notification, the entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.
Penalties/Private Cause of Action	For violations of this section, the Attorney General is empowered to bring an action in law or equity to address violations of this section and for other relief that may be appropriate.

Kentucky	
Statute	Ken. Rev. Stat. § 365.732
Covered Entity	Any person or sole proprietorship, partnership, corporation, limited liability company, association, or other entity, however organized and whether or not organized to operate at a profit, that conducts business in Kentucky.
Personal Information Defined	An individual's first name or first initial and last name in combination with any one (1) or more of the following data elements, when the name or data element is not redacted: (i) Social Security number; (ii) Driver's license number; or (iii) Account number or credit or debit card number, in combination with any required security code, access code, or password to permit access to an individual's financial account.
What Triggers Notice Requirement	"Breach of the security of the system" means unauthorized acquisition of unencrypted and unredacted computerized data that compromises the security, confidentiality, or integrity of personally identifiable information maintained by the entity as part of a database regarding multiple individuals that actually causes, or is leads the entity to reasonably believe has caused or will cause, identity theft or fraud against any resident of Kentucky. Any breach shall be disclosed following discovery or notification of the breach.
Encryption/Redaction Safe Harbor	Notification is not required if the accessed personal information was encrypted or the data element is redacted.
Exemptions from Notification	Notification not required if the incident does not cause, or lead the entity to reasonably believe has caused or will cause, identity theft or fraud to a resident of Kentucky.
Timing of Notification	Notification must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement regarding any impediment to a criminal investigation or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. Notification may be delayed if law enforcement determines that notification will impede a criminal investigation. If notification is made to more than 1000 people at one time, the entity shall notify, without unreasonable delay, all consumer reporting agencies and credit bureaus that compile and maintain files on consumers on a nationwide basis.
Penalties/Private Cause of Action	N/A

Louisiana	
Statute	La. R.S. § 51:3071 *et seq.* La. Admin. Code tit. 16, § 701
Covered Entity	Any individual, corporation, partnership, sole proprietorship, joint stock company, joint venture, or any other legal entity that conducts business in Louisiana or that owns or licenses computerized data that includes personal information.
Personal Information Defined	The first name or first initial and last name of an individual resident of this state in combination with any one or more of the following data elements, when the name or the data element is not encrypted or redacted: (i) Social security number. (ii) Driver's license number or state identification card number. (iii) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. (iv) Passport number. (v) 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.
What Triggers Notice Requirement	"Breach of the security system" means 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 personal information. After the entity discovers a breach in the security of the system containing such data, it must notify any Louisiana resident whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
Encryption Safe Harbor	Notification is not required if the accessed personal information was encrypted or redacted.
Exemptions from Notification	Notification is not required if, after a reasonable investigation, it is determined that there is no reasonable likelihood of harm to customers. A copy of this written determination must be maintained for five years.
Timing of Notification	Notification of breach must be provided in the most expedient time possible and without unreasonable delay, but not later than 60 days from the discovery of the breach, consistent with the legitimate needs of law enforcement and any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data. Notification may be delayed by law enforcement if it will impede a

Louisiana	
	criminal investigation. When notification is delayed, the person shall provide the attorney general with the reasons for the delay, in writing, within the sixty day notification period. When notification is required to individuals, notification must also be provided to the consumer protection section of the attorney general's office within 10 days of distribution of the notice to the individuals.
Penalties/Private Cause of Action	A violation of this statute shall constitute an unfair act or practice pursuant to La. R.S. 51:1405(A). 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 personal information. Failure to provide timely notice to the attorney general may be punishable by a fine not to exceed $5000 per violation. Each day notice is not received by the attorney general is a separate violation.

Maine	
Statute	10 Me. Rev. Stat. §§ 1346 *et seq.*
Covered Entity	A person who, for monetary fees or dues, engages in whole or in part in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring or communicating information concerning individuals for the primary purpose of furnishing personal information to nonaffiliated 3rd parties, and that maintains computerized data that includes personal information becomes aware of a breach of the security of the system.
Personal Information Defined	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: (i) Social security number; (ii) Driver's license number or state identification card number; (iii) 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; (iv) Account passwords or personal identification numbers or other access codes; or (v) Any of the data elements contained in paragraphs A to D when not in connection with the individual's first name, or first initial, and last name, if the information if compromised would be sufficient to permit a person to fraudulently assume or attempt to assume the identity of the person whose information was compromised.
What Triggers Notice Requirement	"Security breach" or "breach of the security of the system" means the unauthorized acquisition, release or use of an individual's computerized data that includes personal information that compromises the security, confidentiality, or integrity of personal information. When the entity becomes aware of a breach of the security of the system, it must conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused. The entity shall give notice of a breach of the security of the system, following discovery or notification of the breach, to a Maine resident whose information has been, or is reasonably believed to have been, acquired by an unauthorized person.
Encryption/Redaction Safe Harbor	Notification is not required if the accessed personal information was encrypted or redacted.
Exemptions from Notification	Notification is not required if, after conducting a good faith, reasonable, and prompt investigation, the entity determines that

Maine	
	there is no reasonable likelihood that the personal information has or will be acquired by an unauthorized person.
Timing of Notification	Notification of breach must be provided in the most expedient time possible and without unreasonable delay, but no more than 30 days after the entity becomes aware of the breach and identifies its scope, consistent with the legitimate needs of law enforcement and any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the system. Delay of Notification for Criminal Investigation: Notification may be delayed no longer than seven business days after a law enforcement agency determines that the notification will not compromise a criminal investigation. A person must also notify appropriate state regulators within the Department of Professional and Financial Regulation, or if the person is not regulated by the department, the attorney general. If notification is required to more than 1000 people at a single time, the entity must notify, without unreasonable delay, the consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.
Penalties/Private Cause of Action	A person that violates this chapter commits a civil violation and is subject to one or more of the following: a fine of not more than $500 per violation, up to a maximum of $2,500 for each day the person is in violation of this chapter; equitable relief; or enjoinment from further violations of this chapter. The appropriate state regulators within the Department of Professional and Financial Regulation shall enforce this chapter for any person that is licensed or regulated by those regulators. The Attorney General shall enforce this chapter for all other persons.

Maryland	
Statute	Md. Com. Law Code §§ 14-3501 *et seq.*
Covered Entity	A sole proprietorship, partnership, corporation, association, or any other business entity, whether or not organized to operate at a profit that owns or, licenses, or maintains computerized data that includes personal information of an individual residing in the State.
Personal Information Defined	An individual's first name or first initial and last name in combination with any one or more of the following data elements, when the name or the data elements are not encrypted, redacted, or otherwise protected by another method that renders the information unreadable or unusable: (i) A Social Security number, an Individual Taxpayer Identification Number, a passport number, or other identification number issued by the federal government; (ii) A driver's license number or State identification card number; (iii) An account number, a credit card number, or a debit card number, in combination with any required security code, access code, or password, that permits access to an individual's financial account; (iv) Health information or, any information created by an entity covered by the federal Health Insurance Portability and Accountability Act of 1996 regarding an individual's medical history, medical condition, or medical treatment or diagnosis, including information about an individual's mental health; (v) A 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 (vi) 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. A user name or e-mail address in combination with a password or security question and answer that permits access to an individual's e-mail account.
What Triggers Notice Requirement	"Breach of the security of a system" means the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a business. When the entity discovers or is notified of a breach it must conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information of the individual

Maryland	
	has been or will be misused. If this investigation determines that the misuse of the individual's personal information has occurred or is reasonably likely to occur, the entity must notify the individual.
Encryption/Redaction Safe Harbor	Notification is not required if the accessed personal information was encrypted, redacted, or otherwise protected by another method that rendered the information unreadable or unusable.
Exemptions from Notification	Notification is not required if, after a good faith, reasonable, and prompt investigation the entity determines that the personal information 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 must maintain records reflecting this determination for 3 years.
Timing of Notification	Notification must be made as soon as reasonably practicable after the entity conducts its investigation, but not later than 45 days after the business concludes the investigation. It may be delayed during the investigation to determine the scope of the breach, identify the individuals affected, or restore the integrity of the system. Notification may be delayed if law enforcement determines that it will impede a criminal investigation or jeopardize national or homeland security. If notice is delayed because of law enforcement, notification must be given as soon as reasonably practicable but no later than 30 days after the law enforcement agency determines it will not impede a criminal investigation and will not jeopardize homeland or national security. Before giving notice to individuals the entity must provide notice to the office of the attorney general. If notification is made to 1000 or more individuals, the entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.
Penalties/Private Cause of Action	A violation of this statute is an unfair or deceptive trade practice. And is subject to the enforcement and penalty provisions contained in Title 13 of Maryland Commercial Law.

Massachusetts	
Statute	Mass. Gen. Laws ch. 93H, § 1 *et seq.*
Covered Entity	A person or agency that owns or licenses data that includes personal information about a resident of Massachusetts.
Personal Information Defined	A resident's first name and last name or first initial and last name in combination with any 1 or more of the following data elements that relate to such resident: (i) Social Security number; (ii) driver's license number or state-issued identification card number; or (iii) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account. Data is any material upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics.
What Triggers Notice Requirement	"Breach of security" means the 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 personal information, that creates a substantial risk of identity theft or fraud against a Massachusetts resident. An entity must provide notice as soon as practicable and without unreasonable delay once the entity (1) knows or has reason to know of a breach of security or (2) knows or has reason to know that the personal information of a resident was acquired or used by an unauthorized person or used for an unauthorized purpose to the attorney general, the director of consumer affairs and business regulation, and the affected resident.
Encryption/Redaction Safe Harbor	Notification is not required if the accessed data was encrypted, and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of the personal information was not acquired.
Exemptions from Notification	Notification is required only if the breach creates a substantial risk of identity theft or fraud against a Massachusetts resident or when the entity knows or has reason to know that the resident's personal information was acquired or used by an unauthorized person or used for an unauthorized purpose.
Timing of Notification	Notice must be given as soon as practicable and without unreasonable delay to the attorney general, the director of consumer affairs and business regulation, and the affected resident. Notice may be delayed at the request of law enforcement agencies if it is determined that

Massachusetts	
	notification will impede a criminal investigation and the agency has notified the attorney general in writing of the determination. Upon receipt of this notice, the director of consumer affairs and business regulation shall identify any relevant consumer reporting agency or state agency, as deemed appropriate by said director, and forward the names of the identified consumer reporting agencies and state agencies to the notifying person or agency. Such person or agency shall, as soon as practicable and without unreasonable delay, also provide notice, in accordance with this chapter, to the consumer reporting agencies and state agencies identified by the director of consumer affairs and business regulation. 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 this statute.
Penalties/Private Cause of Action	The Attorney General may bring an action against a person or otherwise to remedy violations of this chapter and for other relief that may be appropriate under section 4 of Mass. Gen. Laws. ch. 93A.

Michigan	
Statute	Mich. Comp. Laws §§ 445.63, 445.72
Covered Entity	An individual, partnership, corporation, limited liability company, association, or other legal entity or agency that owns or licenses data that are included in a database that discovers a security breach.
Personal Information Defined	The first name or first initial and last name linked to 1 or more of the following data elements of a resident of this state: (i) Social security number. (ii) Driver license number or state personal identification card number. (iii) Demand deposit or other financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to any of the resident's financial accounts.
What Triggers Notice Requirement	"Security breach" or "breach of the security of a database" means the unauthorized access and acquisition of data that compromises the security or confidentiality of personal information regarding multiple individuals. When the entity discovers or receives notice of a security breach, it must notify the affected Michigan resident if that resident's (1) unencrypted and unredacted personal information was accessed and acquired by an unauthorized person; or (2) personal information was accessed and acquired in encrypted form by a person with unauthorized access to the encryption key.
Encryption/Redaction Safe Harbor	Notification is not required if the accessed personal information was encrypted or redacted, and the unauthorized user did not have the encryption key.
Exemptions from Notification	Notice is not required if it is determined that the 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 Michigan residents.
Timing of Notification	Notice must be given without unreasonable delay. Notice may be delayed for an investigation to determine the scope of the security breach and restore reasonable integrity of the system. Notice may also be delayed at the request of law enforcement if law enforcement determines that notification will impede a criminal or civil investigation or jeopardize homeland or national security.
Penalties/Private Cause of Action	A person that knowingly fails to provide any notice of a security breach may be ordered to pay a civil fine of not more than $250 for each failure to provide notice. The Attorney General or a prosecuting attorney may bring an action to recover a civil fine. The aggregate liability for civil fines for multiple violations shall not exceed $750,000.

Minnesota	
Statute	Minn. Stat. § 325E.61
Covered Entity	Any person or business that conducts business in this state, and that owns or licenses data that includes personal information.
Personal Information Defined	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: (i) Social Security number; (ii) driver's license number or Minnesota identification card number; or (iii) 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.
What Triggers Notice Requirement	"Breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. The entity must disclose any breach of the security of the system, following discovery or notification of the breach, to any resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
Encryption/Redaction Safe Harbor	Notification not required if the accessed personal information was encrypted or secured by another method of technology that makes the data unreadable or unusable, or was secured and the encryption key, password, or other means necessary for reading or using the data was not also acquired: social security number, driver's license number or Minnesota identification number, or 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
Exemptions from Notification	These statutes do not apply to any "financial institution," as defined by 15 U.S.C. § 6809(3).
Timing of Notification	Notification of a breach must be provided 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, security, and confidentiality of the system. Notice can be delayed if instructed by law enforcement agencies if it will impede a criminal investigation.

Minnesota	
	If more than 500 people must be notified, the person shall also notify, within 48 hours, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.
Penalties/Private Cause of Action	The Attorney General shall enforce this statute under Minn. Stat. § 8.31.

Mississippi	
Statute	Miss. Code § 75-24-29
Covered Entity	Any natural persons, corporations, trusts, partnerships, incorporated and unincorporated associations, and any other legal entity, which conducts business in this state and which, in the ordinary course of the entity's business functions, own, license or maintain personal information of any resident of this state.
Personal Information Defined	An individual's first name or first initial and last name in combination with any one or more of the following data elements: (i) Social security number; (ii) Driver's license number or state identification card number; or (iii) An 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.
What Triggers Notice Requirement	"Breach of security" means unauthorized acquisition of electronic files, media, databases, or computerized data containing personal information of any Mississippi resident when access to the personal information has not been secured by encryption or any other method or technology that renders the personal information unreadable or unusable. A breach of security must be disclosed to all affected individuals.
Encryption/Redaction Safe Harbor	Notification is not required if the accessed personal information was encrypted or made unreadable or unusable by some other method or technology.
Exemptions from Notification	Notification is not required if, after an appropriate investigation, it is reasonably determined that the breach will not likely result in harm to the affected individuals.
Timing of Notification	Notification must be made without unreasonable delay, subject to the needs of law enforcement and the completion of an investigation to determine the nature and scope of the incident, to identify the affected individuals, or to restore the reasonable integrity of the data system. Notification may also be delayed if the law enforcement agency determines that notification will impede a criminal investigation or national security.
Penalties/Private Cause of Action	Failure to comply with the requirements of this section shall constitute an unfair trade practice and shall be enforced by the Attorney General; however, nothing in this statute may be construed to create a private right of action.

Missouri	
Statute	Mo. Rev. Stat. § 407.1500
Covered Entity	Any individual, corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture, government, governmental subdivision, governmental agency, governmental instrumentality, public corporation, or any other legal or commercial entity that owns or licenses personal information of residents of Missouri or any person that conducts business in Missouri that owns or licenses personal information in any form of a resident of Missouri.
Personal Information Defined	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: (i) Social Security number; (ii) Driver's license number or other unique identification number created or collected by a government body; (iii) 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 an individual's financial account; (iv) 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; (v) Medical information, including any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or (vi) Health insurance information, including a n individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual.
What Triggers Notice Requirement	"Breach" or "breach of security" means unauthorized access to and unauthorized acquisition of personal information maintained in computerized form by a person that compromises the security, confidentiality, or integrity of the personal information. The entity must notify the affected consumer that there has been a breach after discovery of the breach.
Encryption/Redaction Safe Harbor	Notification is not required 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.

Missouri	
Exemptions from Notification	Notification is not required if, after appropriate investigation or consultation with the relevant responsible law enforcement agency, it is determined that a risk of identity theft or other fraud to any consumer is not reasonably likely to occur because of the breach. This determination must be documented in writing and kept for five years.
Timing of Notification	Notice must be made without unreasonable delay, consistent with the needs of law enforcement, 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. Notice may be delayed by law enforcement if law enforcement informs the entity that the notification may impede a criminal investigation, or jeopardize national or homeland security, provided the request is made in writing.
Penalties/Private Cause of Action	The 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.

Montana	
Statute	Mont. Code §§ 30-14-1701–02 & 1704
Covered Entity	Any person or sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the law of this state, any other state, the United States, or any other country or the parent or the subsidiary of a financial institution, that conducts business in Montana and that owns or licenses computerized data that includes personal information.
Personal Information Defined	"Personal Information" means a Montana resident's first name or first initial and last name in combination with any of the following, when either the name or data elements are not encrypted: (i) Social security number; (ii) Driver's license number, a state identification card number, a tribal identification number; (iii) Account number or credit 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; (iv) Medical record information as relates to an individual's physical or mental condition, medical history, medical claims history, or medical treatment and is obtained from a medical professional or medical care institution, from the individual, or from the individual's spouse, parent, or legal guardian; (v) taxpayer identification number; or (vi) an identity protection personal identification number issued by the United States Internal Revenue Service.
What Triggers Notice Requirement	"Breach of the security of the data system" means unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information and causes or is reasonably believed to cause loss or injury to a Montana resident. A breach must be disclosed following discovery or notification of the breach to any Montana resident whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person.
Encryption/Redaction Safe Harbor	Notification is not required if the accessed personal information was encrypted.
Exemptions from Notification	Notification not required if the incident has not caused or is not reasonably believed to have caused loss or injury to a Montana resident.

Montana	
Timing of Notification	Notification must be made without unreasonable delay, consistent with the legitimate needs of law enforcement and any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. Notification may be delayed if law enforcement determines notification will impede a criminal investigation and requests a delay. Any person or business that is required to issue a notification pursuant to this section shall notify the attorney general's consumer protection office.
Penalties/Private Cause of Action	Whenever the department has reason to believe that a person has violated this statute and that proceeding would be in the public interest, the department may bring an action in the name of the state against the person to restrain by temporary or permanent injunction or temporary restraining order the use of the unlawful method, act, or practice upon giving appropriate notice to that person under Mont. Code 30-14-111(2). A violation of this statute is a violation of 30-14-103, and the penalties are as provided in 30-14-142.

Nebraska	
Statute	Neb. Rev. Stat. §§ 87-801 *et seq.*
Covered Entity	An individual or corporation, business trust, estate, trust, partnership, limited partnership, limited liability partnership, limited liability company, association, organization, joint venture, government, governmental subdivision, agency, or instrumentality, or any other legal entity, whether for profit or not for profit that owns or licenses computerized data that includes personal information about a resident of Nebraska.
Personal Information Defined	A Nebraska 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: (i) Social security number; (ii) Motor vehicle operator's license number or state identification card number; (iii) Account number or credit 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; (iv) Unique electronic identification number or routing code, in combination with any required security code, access code, or password; or (v) Unique biometric data, such as a fingerprint, voice print, or retina or iris image, or other unique physical representation. A user name or email address, in combination with a password or security question and answer, that would permit access to an online account.
What Triggers Notice Requirement	"Breach of the security of the system" means the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a commercial entity. When the entity becomes aware of a breach of the security of the system, it must conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be used for an unauthorized purpose. If the investigation determines that the use of information about a Nebraska resident for an unauthorized purpose has occurred or is reasonably likely to occur, the entity must notify the affected resident and the state attorney general.
Encryption/Redaction Safe Harbor	Notification is not required if the accessed personal information was encrypted, redacted, or otherwise altered in a way that made it

Nebraska	
	unreadable. Information is not considered encrypted if the encryption key or process is reasonably believed to have been acquired in the breach.
Exemptions from Notification	Notification is not required if the entity determines that the use of information about the affected Nebraska resident for an unauthorized purpose has not occurred or is not reasonably likely to occur.
Timing of Notification	Notification must be provided as soon as possible and without unreasonable delay, consistent with measures necessary to determine scope of the breach and restore reasonable integrity of the computerized data system. Notice can be delayed if instructed by law enforcement, if it will impede a criminal investigation. Notice must also be provided to the attorney general no later than when notice is provided to the individuals.
Penalties/Private Cause of Action	The Attorney General may issue subpoenas and seek and recover direct economic damages for each affected Nebraska resident.

Nevada	
Statute	Nev. Rev. Stat. §§ 603A.010 *et seq.*
Covered Entity	Any governmental agency, institution of higher education, corporation, financial institution or retail operator or any other type of business entity or association that owns or licenses computerized data which includes personal information.
Personal Information Defined	A natural person's first name or first initial and last name in combination with any one or more of the following data elements, when the name and data elements are not encrypted: (i) Social security number. (ii) Driver's license number, driver authorization card number or identification card number. (iii) Account number, credit card number or debit card number, in combination with any required security code, access code or password that would permit access to the person's financial account. (iv) A medical identification number or a health insurance identification number. (v) A user name, unique identifier or electronic mail address in combination with a password, access code or security question and answer that would permit access to an online account.
What Triggers Notice Requirement	"Breach of the security of the data system" means unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the data collector. A breach must be disclosed to any Nevada resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
Encryption/Redaction Safe Harbor	Notification is not required if the accessed personal information was encrypted.
Exemptions from Notification	N/A
Timing of Notification	Notification must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system data. Notification may be delayed if law enforcement determines notification will impede a criminal investigation. If an entity determines that notification is required to be given pursuant to the provisions of this section to more than 1,000 persons at any one time, it shall also notify, without unreasonable delay, any

Nevada	
	consumer reporting agency that compiles and maintains files on consumers on a nationwide basis.
Penalties/Private Cause of Action	A private right of action exists for the data collector for damages against a person that unlawfully obtained or benefits from personal information obtained from records maintained by the data collector. The Attorney General may bring an action against the person to obtain a temporary or permanent injunction against the violation.

New Hampshire	
Statute	N.H. Rev. Stat. §§ 359-C:19 *et seq.*; 332-I:1 *et seq.*
Covered Entity	**Personal Information Breach Notification Statute**: An individual, corporation, trust, partnership, incorporated or unincorporated association, limited liability company, or other form of entity, or any agency, authority, board, court, department, division, commission, institution, bureau, or other state governmental entity, or any political subdivision of the state doing business in New Hampshire and that owns or licenses computerized data including personal information. **Medical Information Unauthorized Disclosure Notification Statute: A hea**lth care provider or a business associate of a health care provider.
Personal Information Defined	**Personal Information Breach Notification Statute**: "Personal Information" means New Hampshire resident's first name or initial and last name in combination with any of the following data elements, when either the name or the data elements are not encrypted: (i) Social security number; (ii) Driver's license number or other governmental identification number; (iii) 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 Unauthorized Disclosure Notification Statute**: Incorporates definition of protected medical information from §§ 262 and 264 of the Health Insurance Portability and Accountability Act of 1996.
What Triggers Notice Requirement	**Personal Information Breach Notification Statute**: "Security breach" is the unauthorized acquisition of computerized data that compromises the security or confidentiality of personal information maintained by a person doing business in this state. When the entity becomes aware of a security breach, it must promptly determine the likelihood that the information has been or will be misused. If the determination is that misuse of the information has occurred, is reasonably likely to occur, or if a determination cannot be made, the entity must notify the affected individuals as soon as possible. **Medical Information Unauthorized Disclosure Notification Statute**: The statute is triggered by the unauthorized use or disclosure of protected health information for marketing or fundraising purposes. Health care providers may be liable even if such use is permissible under federal law.
Encryption/Redaction Safe Harbor	**Personal Information Breach Notification Statute**: Notification is not required if the accessed personal information was encrypted unless

New Hampshire	
	the encryption key, security code, access code, or password would permit access to the encrypted data.
Exemptions from Notification	**Personal Information Breach Notification Statute**: Notification is not required if it is determined that misuse of the information has not occurred and is not reasonably likely to occur, unless a determination cannot be made, and then notification is required.
Timing of Notification	**Personal Information Breach Notification Statute**: Notice must be made as soon as possible, but may be delayed by a law enforcement agency, or national or homeland security agency if the notification will impede a criminal investigation or jeopardize national or homeland security. The attorney general must be notified before the affected individuals are notified, unless the entity is subject to R.S.A. 358-A:3, in which case, the primary regulatory authority of the entity must be notified. If an entity must notify more than 1000 consumers of a breach, the entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis. **Medical Information Unauthorized Disclosure Notification Statute**: The healthcare provider shall "promptly notify in writing the individual or individuals whose protected health information was disclosed."
Penalties/Private Cause of Action	**Personal Information Breach Notification Statute**: Persons injured because of a violation may bring an action for damages and for such equitable relief, including an injunction, as the court deems necessary and proper. A prevailing plaintiff shall be awarded actual damages, the costs of the suit and reasonable attorney's fees. If the court finds a willful or knowing violation of this chapter, damages will be set at 2 to 3 times the actual damages. In addition, a prevailing plaintiff shall be awarded the costs of the suit and reasonable attorney's fees, as determined by the court. The Attorney General's office shall enforce these provisions pursuant to R.S.A. 358-A:4. **Medical Information Unauthorized Disclosure Notification Statute**: An aggrieved individual whose health records were wrongly disclosed may bring a civil action and, if successful, shall be awarded special or general damages of not less than $1,000 for each violation, and costs and reasonable legal fees.

New Jersey	
Statute	N.J. Stat. §§ 56:8-161; 56:8-163–66
Covered Entity	Any sole proprietorship, partnership, corporation, association, or other entity, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the law of this State, any other state, the United States, or of any other country, or the parent or the subsidiary of a financial institution, that conducts business in New Jersey, or any public entity that compiles or maintains computerized records that include personal information.
Personal Information Defined	An individual's first name or first initial and last name linked with any one or more of the following data elements: (i) Social Security number; (ii) driver's license number or State identification card number; (iii) 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; or (iv) user name, email address, or any other account holder identifying information, in combination with any password or security question and answer that would permit access to an online account. (Note: (iv) is effective as of September 1, 2019.) Dissociated data that, if linked, would constitute personal information is personal information if the means to link the dissociated data were accessed in connection with access to the dissociated data.
What Triggers Notice Requirement	"Breach of security" means unauthorized access to electronic files, media or data containing personal information that compromises the security, confidentiality or integrity of personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable. The entity must notify New Jersey resident customers of any breach of security of those computerized records following discovery or notification of the breach, if that customer's personal information was, or is reasonably believed to have been, accessed by an unauthorized person.
Encryption/Redaction Safe Harbor	Notification is not required if the accessed personal information was encrypted or made unreadable or unusable by some other method or technology.
Exemptions from Notification	Notification is not required if it is established that misuse of the information is not reasonably possible. Any determination shall be documented in writing and retained for five years.

New Jersey	
Timing of Notification	Notification must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. Notification may be delayed if a law enforcement agency determines that the notification will impede a criminal or civil investigation. In advance of the disclosure to the customer, the entity must 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. In the event that more than 1000 people must be notified at one time, the entity must also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.
Penalties/Private Cause of Action	It is an unlawful practice and a violation of N.J. Stat. §§ 56:8-1, *et seq.* to willfully, knowingly or recklessly violate this statute.

New Mexico	
Statute	N.M. Stat. §§ 57-12C-1 *et seq.*
Covered Entity	A person that owns or licenses elements that include personal identifying information of a New Mexico resident.
Personal Information Defined	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: (i) social security number; (ii) driver's license number; (iii) government-issued identification number; (iv) 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 (v) biometric data (a record generated by automatic measurements of an identified individual's fingerprints, voice print, iris or retina patterns, facial characteristics or hand geometry that is used to uniquely and durably authenticate an individual's identity when the individual accesses a physical location, device, system or account).
What Triggers Notice Requirement	"Security breach" means the 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 personal identifying information maintained by a person. An entity must notify New Mexico residents if their personal identifying information is reasonably believed to have been subject to a security breach.
Encryption/Redaction Safe Harbor	Notification is not required if the information was encrypted or redacted or otherwise rendered unreadable or unusable.
Exemptions from Notification	Notification to affected New Mexico residents is not required if, after an appropriate investigation, the person 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 if a law enforcement agency determines that notification will impede a criminal investigation or as necessary to determine the scope of the security breach and restore the reasonable integrity, security and confidentiality of the data system.

New Mexico	
	An entity that must notify more than 1000 residents as a result of a single breach must also notify the office of the attorney general and major consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, in the most expedient time possible but no later than 45 calendar days.
Penalties/Private Cause of Action	When the attorney general has a reasonable belief that a violation of the Data Breach Notification Act has occurred, the attorney general may bring an action on the behalf of individuals and in the name of the state alleging a violation of that act. The court may issue an injunction and award damages for actual costs or losses, including consequential financial losses. If the court determines that a person violated the statute knowingly or recklessly, the court may impose a civil penalty of the greater of $25,000 or, in the case of failed notification, $10.00 per instance of failed notification up to a maximum of $150,000.

New York	
Statute	N.Y. Gen. Bus. Law § 899-aa
Covered Entity	Any person or business which owns or licenses computerized data which includes private information of a New York resident.
Personal Information Defined	The law applies to "private information," which means either: (i) personal information consisting of 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: (1) social security number; (2) driver's license number or non-driver identification card number; (3) account number, credit or debit card number, in combination with any required security code, access code, password or other information that would permit access to an individual's financial account; (4) 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 (5) biometric information, meaning data generated by electronic measurements of an individual's unique physical characteristics, such as a 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. (ii) a user name or e-mail address in combination with a password or security question and answer that would permit access to an online account. Personal Information means any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person.
What Triggers Notice Requirement	"Breach of the security of the system" shall mean 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, by an unauthorized person or a person without valid authorization, such business may

New York

	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, such business may consider the following factors, among others: (i) 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; or (ii) indications that the information has been downloaded or copied; or (iii) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported. An entity shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of New York state whose private information was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization.
Encryption/Redaction Safe Harbor	Notification is not required when the accessed "private information" was encrypted and the encryption key was not accessed or acquired.
Exemptions from Notification	Notice to affected persons under this section is not required if the exposure of private information was an inadvertent disclosure by persons authorized to access private information, and the person or business 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 - a user name or e-mail address in combination with a password or security question and answer that would permit access to an online account. Such a determination must be documented in writing and maintained for at least five years. If the incident affects over five hundred residents of New York, the person or business shall provide the written determination to the state attorney general within ten days after the determination.
Timing of Notification	Notification of a breach must be provided in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and to restore the integrity of the system. Notice can be delayed if instructed by law enforcement agencies that notification will impede a criminal investigation.

New York	
	In the event notification of New York residents are required, the entity must also notify the attorney general, department of state. This notification should not delay notice of New York residents. If more than 5000 New York residents are notified at one time, the entity shall notify consumer reporting agencies without delaying notice to affected New York residents.
Penalties/Private Cause of Action	The Attorney General may bring an action in a court having jurisdiction to issue an injunction. The court may award damages for actual costs or losses incurred by a person entitled to notice. Whenever the court determines that a person or business violated this article knowingly or recklessly, the court may impose a civil penalty of the greater of $5,000 or up to $20 per instance of failed notification, but the latter amount shall not exceed $250,000. Any other lawful remedy available can be sought as long as such action is commenced within three years after either the date on which the attorney general became aware of the violation, or the date of notice sent pursuant to paragraph (a) of subdivision eight of this section, whichever occurs first. In no event shall an action be brought after six years from the date of discovery of the breach of private information by the company unless the company took steps to hide the breach.

North Carolina	
Statute	N.C. Gen. Stat. §§ 75-61, 75-65
Covered Entity	Any sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not organized to operate at a profit or any financial institution that owns or licenses personal information of residents of North Carolina or any business that conducts business in North Carolina that owns or licenses personal information in any form (whether computerized, paper, or otherwise).
Personal Information Defined	A person's first name or initial and last name, combined with one or more of the following: (i) Social security or employer taxpayer identification numbers. (ii) Driver's license, State identification card, or passport numbers. (iii) Checking account numbers. (iv) Savings account numbers. (v) Credit card numbers. (vi) Debit card numbers. (vii) Personal Identification (PIN) Code as defined in G.S. 14-113.8(6). (viii) Digital signatures. (ix) Any other numbers or information that can be used to access a person's financial resources. (x) Biometric data. (xi) Fingerprints. (xii) Passwords if they would permit access to a person's financial account or resources.
What Triggers Notice Requirement	"Security breach" means an incident of unauthorized access to and acquisition of unencrypted and unredacted records or data containing personal information where illegal use of the personal information has occurred or is reasonably likely to occur or that creates a material risk of harm to a consumer. The entity must notify affected individuals when it discovers or is notified of a security breach.
Encryption/Redaction Safe Harbor	Notification is not required when the accessed personal information was encrypted, unless there is unauthorized access to encrypted records along with the confidential process or key.
Exemptions from Notification	Notification is not required where illegal use of the personal information has not occurred or is not reasonably likely to occur or where there is no material risk of harm to a consumer.

North Carolina

Timing of Notification	Notification shall be made without unreasonable delay, consistent with the legitimate needs of law enforcement and 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. Notice may 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. The entity must also notify without unreasonable delay, the Consumer Protection Division of the Attorney General's Office. If notice is provided to more than 1000 people at one time, the entity shall notify, without unreasonable delay, the Consumer Protection Division of the Attorney General's Office and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.
Penalties/Private Cause of Action	A violation of this statute is a violation of G.S. 75-1.1. No private right of action may be brought by an individual for a violation of this statute unless he or she is injured because of the violation.

North Dakota	
Statute	N.D. Cent. Code §§ 51-30-01 *et seq.*
Covered Entity	Any person that owns or licenses computerized data that includes personal information.
Personal Information Defined	"Personal information" means an individual's first name or first initial and last name combined with any of the following data elements, when the name and the data elements are not encrypted: (i) the individual's social security number; (ii) the operator's license number assigned by the department of transportation; (iii) a non-driver color photo identification card number assigned by the department of transportation; (iv) the individual's financial institution account number, credit card number, or debit card number combined with any required security code, access code, or password that would permit access to an individual's financial accounts; (v) the individual's date of birth; (vi) the maiden name of the individual's mother; (vii) medical information (any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional); (viii) health insurance information (an individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual); (ix) an identification number assigned to the individual by the individual's employer combined with any required security code, access code, or password; or (x) the individual's digitized or other electronic signature.
What Triggers Notice Requirement	"Breach of the security system" means unauthorized acquisition of computerized data when access to personal information has not been secured by encryption or by another method that renders the electronic files, media, or databases unreadable or unusable. The entity must disclose a breach of the security system, following discovery or notification of the breach, to any North Dakota resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
Encryption/Redaction Safe Harbor	Notification is not required when the accessed personal information was encrypted.
Exemptions from Notification	N/A

North Dakota	
Timing of Notification	Notification of a breach must be provided in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system. Notice can be delayed if instructed by law enforcement agencies that notification will impede a criminal investigation. The entity must also disclose a breach to the attorney general which effects more than 250 individuals.
Penalties/Private Cause of Action	The Attorney General may enforce this statute under Chapter 51-15 and may seek all applicable remedies under that Chapter.

Ohio	
Statute	Ohio Rev. Code Ann. §§ 1349.19
Covered Entity	Any individual, corporation, business trust, estate, trust, partnership, and association that owns or licenses computerized data that includes personal information, except only business entities that conduct business in Ohio.
Personal Information Defined	An Ohio resident'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: (i) social security number; (ii) driver's license number or state identification number; (iii) account number or credit 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.
What Triggers Notice Requirement	"Breach of the security system" means the unauthorized access to and acquisition of computerized data that compromises the security or confidentiality of personal information owned or licensed by a person 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 a resident of this state. The entity must disclose any breach of the security system, following its discovery or notification of the breach, to any Ohio resident whose personal information was, or is reasonably believed to have been, accessed and acquired by an unauthorized person if the access and acquisition by the unauthorized person causes, or it is reasonably believed that it will cause, a material risk of identity theft or other fraud to the resident.
Encryption/Redaction Safe Harbor	Notification is not required when the accessed personal information was encrypted, redacted, or altered in a way that made it unreadable.
Exemptions from Notification	Notification is required only if the access and acquisition by the unauthorized person causes, or it is reasonably believed that it has or will cause, a material risk of identity theft or other fraud to the affected resident.
Timing of Notification	Notice must be provided in the most expedient time possible but no later than 45 days following discovery or notification of the breach, subject to the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach, including which residents' personal information was accessed and acquired, and to restore the reasonable integrity of the data system.

Ohio	
	Notification may be delayed if a law enforcement agency determines that the disclosure or notification will impede a criminal investigation or jeopardize homeland or national security. Notification to all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis is required if more than 1000 Ohio residents are notified following a single occurrence of a breach. This shall not delay notification to individuals.
Penalties/Private Cause of Action	The Attorney General may investigate any violations of these sections and bring an action to collect a civil penalty against a person or agency for failing to comply with the statute.

Oklahoma	
Statute	Okla. Stat., tit. 24 § 161 *et seq*
Covered Entity	A natural person or corporations, business trusts, estates, partnerships, limited partnerships, limited liability partnerships, limited liability companies, associations, organizations, joint ventures, governments, governmental subdivisions, agencies, or instrumentalities, or any other legal entity, whether for profit or not-for-profit, that owns or licenses computerized data that includes personal information.
Personal Information Defined	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 this state, when the data elements are neither encrypted nor redacted: (i) social security number; (ii) driver's license number or state identification number; (iii) account number or credit 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.
What Triggers Notice Requirement	"Breach of the security system" means the unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an entity as part of a database of personal information regarding multiple individuals and that causes, or it is reasonably believed that it has or will cause, identity theft or other fraud to an Oklahoma resident. The entity must disclose any breach of the security system, following discovery or notification of the breach, to any Oklahoma resident whose unencrypted and unredacted personal information was, or is reasonably believed to have been, accessed and acquired by an unauthorized person and that causes, or it is reasonably believed that it has or will cause, identity theft or other fraud to the resident.
Encryption/Redaction Safe Harbor	Notification is not required if the accessed personal information was encrypted or redacted unless the 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 this state.
Exemptions from Notification	Notification is only required if the entity reasonably believes that the breach has caused or will cause identity theft or other fraud to any Oklahoma resident.

Oklahoma	
Timing of Notification	Notification must be made without unreasonable delay consistent with the need to take any measure to determine the scope of the breach and to restore the reasonable integrity of the system. Notice may be delayed if a law enforcement agency determines and advises that notice will impede a criminal or civil investigation or homeland or national security.
Penalties/Private Cause of Action	A violation that results in injury or loss to Oklahoma residents may be enforced by the Attorney General or a district attorney in the same manner as an unlawful practice under the Oklahoma Consumer Protection Act. The Attorney General or a district attorney shall have exclusive authority to bring an action and may obtain either actual damages or a civil penalty not to exceed $150,000 per breach of the security of the system or series of breaches of a similar nature that are discovered in a single investigation.

Oregon	
Statute	Or. Rev. Stat. § 646A.600 *et seq.*
Covered Entity	An individual, private or public corporation, partnership, cooperative, association, estate, limited liability company, organization or other entity, whether or not organized to operate at a profit, or a public body that owns, licenses, maintains, stores, manages, collects, processes, acquires or otherwise possesses personal information in the course of the person's business, vocation, occupation or volunteer activities, unless the person acts solely as a vendor (note that separate requirements exist for vendors with respect to notification. Please see language of statute for further information.)
Personal Information Defined	A consumer's first name or first initial and last name combined with any one or more of the following data elements, when the data elements are not rendered unusable through encryption, redaction, or other methods, or when the data elements are encrypted and the encryption key has also been acquired: (i) Social Security number (ii) driver license number, or state identification card number issued by the Department of Transportation; (iii) passport number or other United States issued identification number; (iv) 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 consumer'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; (v) data from 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 transaction or other transaction; (vi) a consumer's health insurance policy number or health insurance subscriber identification number combined with any other unique identifier that a health insurer uses to identify the consumer; or (vii) 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. A user name 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 user name or means of identification. Personal information also includes any of the data elements or any combination of the data elements described above when not

Oregon	
	combined with the consumer's user name or the consumer's first name or first initial and last name if (i) encryption, redaction or other methods have not rendered the data element or combination of data elements unusable; and (ii) The data element or combination of data elements would enable a person to commit identity theft against a consumer.
What Triggers Notice Requirement	"Breach of security" means an unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information that a person maintains or possesses. The entity must give notice of the breach of security to any consumer whose personal information was included in the breached information. Before providing notice, the entity shall undertake reasonable measures that are necessary to: (i) Determine sufficient contact information for the intended recipient of the notice; (ii) Determine the scope of the breach of security; and (iii) Restore the reasonable integrity, security and confidentiality of the personal information.
Encryption/Redaction Safe Harbor	Notification is not required if the accessed personal information was encrypted, redacted, or otherwise unusable. Notification is required for encrypted data if the encryption key was acquired.
Exemptions from Notification	Notification is not required if, after investigation and consultation with authorities, the entity determines there is no reasonable likelihood of harm to the person whose information was acquired. This determination must be in writing and kept for five years.
Timing of Notification	Notification must be made in the most expeditious manner possible and without unreasonable delay, but not later than 45 days after the entity discovers the breach or receives notice of the breach. Notification must be consistent with the legitimate needs of law enforcement, if notification will impede a criminal investigation and the law enforcement agency requests in writing the delay. Notification must also be made to the attorney general if the number of individuals to be noticed exceeds 250. Notification must also be made to all consumer reporting agencies that compile and maintain reports on consumers on a nationwide basis, without unreasonable delay, if more than 1000 residents are notified.
Penalties/Private Cause of Action	A person's violation of a provision of this statute is an unlawful practice. In addition to other penalties and enforcement provisions provided by law, any person who violates, or who procures, aids or abets in a

Oregon	
	violation of, the data breach notification law shall be subject to a penalty of not more than $1,000 per violation, but no more than $500,000 total, which shall be paid to the General Fund of the State Treasury. A covered entity in an action or proceeding may affirmatively defend against an allegation that the covered entity or vendor has not developed, implemented and maintained reasonable safeguards to protect the security, confidentiality and integrity of personal information that is subject to this statute.

Pennsylvania	
Statute	73 Pa. Stat. § 2301 *et seq.*
Covered Entity	An individual or sole proprietorship, partnership, corporation, association or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered or holding a license or authorization certificate under the laws of this Commonwealth, any other state, the United States or any other country, or the parent or the subsidiary of a financial institution, doing business in Pennsylvania that maintains, stores or manages computerized data that includes personal information.
Personal Information Defined	"Personal Information" means a Pennsylvania resident's first name or first initial and last name in combination with and linked to any of the following data elements when the data elements are not encrypted or redacted: (i) social security number; (ii) driver's license number or state identification card number; (iii) financial account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account.
What Triggers Notice Requirement	"Breach of the security of the system" means the unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of personal information maintained by the entity as part of a database of personal information regarding multiple individuals and that causes or the entity reasonably believes has caused or will cause loss or injury to any resident of Pennsylvania. The entity must provide notice of any breach of the security of the system, following discovery of the breach, to any resident whose unencrypted and unredacted personal information was, or is reasonably believed to have been, accessed and acquired by an unauthorized person.
Encryption/Redaction Safe Harbor	Notification is not required if the accessed personal information was encrypted or redacted. Notice is required, however, if encrypted information is accessed and acquired in an unencrypted form, if the security breach is linked to a breach of the encryption security, or if the security breach involves a person with access to the encryption key.
Exemptions from Notification	N/A
Timing of Notification	Notification must be made without unreasonable delay, but it may be delayed at the request of law enforcement or in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system.

Pennsylvania	
	Notification may be delayed if a law enforcement agency determines and advises the entity in writing specifically referencing this section that the notification will impede a criminal or civil investigation. Notification must be made to consumer reporting agencies that compile and maintain files on consumers on a nationwide basis if the breach requires notification to more than 1000 people at one time.
Penalties/Private Cause of Action	The Attorney General has exclusive authority to bring an action under the Unfair Trade Practices and Consumer Protection Law for a violation of this act.

Rhode Island	
Statute	R.I. Gen. Laws § 11-49.3-1 *et seq.*
Covered Entity	Any individual, sole proprietorship, partnership, association, corporation, joint venture, business, legal entity, trust, estate, cooperative, or other commercial entity that stores, owns, collects, processes, maintains, acquires, uses, or licenses data that includes personal information.
Personal Information Defined	"Personal information" is an individual's first name or first initial and last name combined with any one or more of the following data elements, when the name and the data elements are not encrypted or are in hard copy paper format: (i) Social security number; (ii) Driver's license number, Rhode Island identification card number, or tribal identification number; (iii) Account, credit, or debit card number combined with any required security code, access code, password or personal identification number that would permit access to an individual's financial account; (iv) Medical information (information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional or provide) or health insurance information (n individual's health insurance policy number, subscriber identification number, or any unique identifier used by a health insurer to identify the individual); or (v) E-mail address with any required security code, access code, or password that would permit access to an individual's personal, medical, insurance or financial account.
What Triggers Notice Requirement	"Breach of the security of the system" means the unauthorized *access or* acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an entity. The entity must provide notification of any disclosure of personal information, or any breach of the security of the system, which poses a significant risk of identity theft to any Rhode Island resident whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person or entity.
Encryption/Redaction Safe Harbor	Notification is not required if the accessed personal information was encrypted.
Exemptions from Notification	Notification is not required if there is not a significant risk of identity theft to any resident whose information was, or reasonably believed to have been, acquired by an unauthorized person or entity.
Timing of Notification	Notification of breach must be made in the most expedient time possible and without unreasonable delay but no later than 45 calendar

Rhode Island	
	days after confirmation of the breach and the ability to ascertain the information required to give notice, consistent with the legitimate needs of law enforcement. Notification can be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. In the event that more than 500 residents are notified, the entity must also notify the attorney general and major credit reporting agencies without delaying notice to the affected residents.
Penalties/Private Cause of Action	Each reckless violation is a civil violation for which a penalty of not more than $100 per occurrence may be adjudged against a defendant. Each knowing and willful violation is a civil violation for which a penalty of not more than $200 per occurrence 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 against the person or business in violation.

South Carolina	
Statute	S.C. Code § 39-1-90
Covered Entity	A natural person, individual or corporation, government or governmental subdivision or agency, trust, estate, partnership, cooperative or association conducting business in this State, and owning or licensing computerized data or other data that includes personal identifying information.
Personal Information Defined	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 this State, when the data elements are neither encrypted nor redacted (i) Social security number; (ii) Driver's license number or state identification card number; (iii) Financial account number, or credit 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 (iv) 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 identify an individual.
What Triggers Notice Requirement	"Breach of the security of the system" means 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 personal identifying information maintained by the person, when illegal use of the information has occurred or is reasonably likely to occur or use of the information creates a material risk of harm to a resident. The entity must notify the affected individuals following discovery or notification of the breach in the security of the data to a resident of this State whose personal identifying information that was not rendered unusable through encryption, redaction, or other methods 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.
Encryption/Redaction Safe Harbor	Notification is not required if the accessed personal information was encrypted, redacted, or rendered unusable through other methods.
Exemptions from Notification	Notification not required if the illegal use of information has not occurred or is not reasonably likely to occur and use of the information does not create a material risk of harm to the resident.
Timing of Notification	Disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with legitimate needs of law

South Carolina	
	enforcement or with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. Notification may be delayed if a law enforcement agency determines that the notification impedes a criminal investigation. If notice is made to more than 1000 people at one time, the entity must also notify, without unreasonable delay, the Consumer Protection Division of the Department of Consumer Affairs and all consumer reporting agencies that compile and maintain files on a nationwide basis.
Penalties/Private Cause of Action	A South Carolina resident injured by a violation may: (i) institute a civil action to recover damages in case of a willful and knowing violation; (ii) institute a civil action that must be limited to actual damages resulting from a violation in case of a negligent violation of this section; (iii) seek an injunction to enforce compliance; and (iv) recover attorney's fees and court costs, if successful. A person who knowingly and willfully violates this section is subject to an administrative fine in the amount of one thousand dollars for each resident whose information was accessible by reason of the breach, the amount to be decided by the Department of Consumer Affairs.

South Dakota	
Statute	S.D.C.L. § 22-40-19 *et seq.*
Covered Entity	Any person or business that conducts business in this state, and that owns or licenses computerized personal or protected information of residents of this state;
Personal Information Defined	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: (i) Social security number; (ii) Driver license number or other unique identification number created or collected by a government body; (iii) Account, credit card, or debit card number, in combination with any required security code, access code, password, routing number, PIN, or any additional information that would permit access to a person's financial account; (iv) Health information as defined in 45 CFR 160.103; or (v) 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. Protected information means: (i) A user name or email address, in combination with a password, security question answer, or other information that permits access to an online account; and (ii) Account number or credit or debit card number, in combination with any required security code, access code, or password that permits access to a person's financial account.
What Triggers Notice Requirement	"Breach of system security" means 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 maintained by the information holder. Following the discovery by or notification to an entity of a breach of system security an information holder shall disclose the breach of system security to any resident of this state whose personal or protected information was, or is reasonably believed to have been, acquired by an unauthorized person.
Encryption/Redaction Safe Harbor	Notification is not required if the data is encrypted and the encryption key is affected by the unauthorized acquisition.

South Dakota	
Exemptions from Notification	An entity is not required to make a disclosure under this section if, following an appropriate investigation and notice to the attorney general, the information holder reasonably determines that the breach will not likely result in harm to the affected person. The information holder shall document the determination under this section in writing and maintain the documentation for not less than three years.
Timing of Notification	A disclosure under this section shall be made not later than sixty days from the discovery or notification of the breach of system security, unless a longer period of time is required due to the legitimate needs of law enforcement if it is determined that notification will impede a criminal investigation. If the notification is delayed, the notification shall be made not later than thirty days after the law enforcement agency determines that notification will not compromise the criminal investigation. Notification must also be made to all consumer reporting agencies and any other credit bureau or agency that compiles and maintains files on consumers on a nationwide basis without unreasonable delay. Notification is required to the attorney general if more than 250 residents are affected.
Penalties/Private Cause of Action	The attorney general may prosecute each failure to disclose under the provisions of this Act as a deceptive act or practice under Section 37-24-6. In addition to any remedy provided under chapter 37-24, the attorney general may bring an action to recover on behalf of the state a civil penalty of not more than ten thousand dollars per day per violation. The attorney general may recover attorney's fees and any costs associated with any action brought under this section.

Tennessee	
Statute	Tenn. Code Ann. §§ 47-18-2105 - 47-18-2107
Covered Entity	Any person or business that conducts business in this state, or any agency of this state or any of its political subdivisions, that owns or licenses computerized personal information of residents of this state.
Personal Information Defined	"Personal Information" means a Tennessee Resident's first name or first initial and last name, in combination with any one or more of the following: (i) Social security number; (ii) Driver's license number; or (iii) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
What Triggers Notice Requirement	"Breach of the security of the system" means the unauthorized acquisition of unencrypted computerized data or encrypted computerized data and the encryption key that materially compromises the security, confidentiality, or integrity of personal information maintained by the entity. The entity must disclose a breach of the security of the system, following discovery or notification of the breach, to any Tennessee resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
Encryption/Redaction Safe Harbor	Notification is not required if the accessed personal information was encrypted unless the encryption key was also compromised.
Exemptions from Notification	N/A
Timing of Notification	The disclosure must be made immediately, but no later than 45 days from the discovery or notification of the breach, consistent with any determination by law enforcement that notification will impede a criminal investigation. If the notification is delayed, it must be made no later than forty-five (45) days after the law enforcement agency determines that notification will not compromise the investigation. If more than 1000 people are notified at one time, the entity must also notify, without unreasonable delay, all consumer reporting agencies and credit bureaus that compile and maintain files on consumers on a nationwide basis.
Penalties/Private Cause of Action	Any violation of this part shall be construed to constitute an unfair or deceptive act or practice affecting trade or commerce. If the attorney general has reason to believe that a person has violated this part, then the attorney general may institute a proceeding under this chapter.

Texas	
Statute	Tex. Bus. & Com. Code §§ 521.002; 521.053; 521.151-152
Covered Entity	A person who conducts business in this state and owns or licenses computerized data that includes sensitive personal information.
Personal Information Defined	The statute applies to "Sensitive Personal Information," which includes an individual's first name or first initial and last name in combination with any of the following, if the name and the items are not encrypted; (i) Social security number; (ii) Driver's license number or government-issued identification number; (iii) Account 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; or information that identifies an individual and relates to: (i) the physical or mental health or condition of the individual; (ii) the provision of health care to the individual; or (iii) payment for the provision of health care to the individual.
What Triggers Notice Requirement	"Breach of system security" means the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt the data. The entity must disclose a breach of system security, after discovering or receiving notification of the breach, to any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
Encryption/Redaction Safe Harbor	Notification is not required if the accessed "sensitive personal information" was encrypted and the key to decrypt was not compromised.
Exemptions from Notification	N/A
Timing of Notification	Notification should be made without unreasonable delay and in each case not later than the 60th day after the date on which the person determines that the breach occurred, except if law enforcement determines that the notification will impede a criminal investigation or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system. If a person is required by this section to notify at one time more than 10,000 persons of a breach of system security, the person shall also

Texas	
	notify each consumer reporting agency that maintains files on consumers on a nationwide basis. A person who is required to disclose or provide notification of a breach of system security under this section shall notify the attorney general of that breach not later than the 60th day after the date on which the person determines that the breach occurred if the breach involves at least 250 residents of this state.
Penalties/Private Cause of Action	The Attorney General may bring a civil suit for damages or an injunction. A person who violates the statute is liable to the state for a civil penalty of at least $2,000 but not more than $50,000 for each violation. A person who fails to take reasonable action to comply with notification requirements is liable to the state for a civil penalty of not more than $100 for each individual to whom notification is due for each consecutive day the person fails to take reasonable action to notify with a maximum penalty of $250,000 for a single breach. If it appears to the attorney general that a person is engaging in, has engaged in, or is about to engage in conduct that violates this chapter, the attorney general may bring an action in the name of the state against the person to restrain the violation by a temporary restraining order or by a permanent or temporary injunction. The attorney general is entitled to recover reasonable expenses, including reasonable attorney's fees, court costs, and investigatory costs, incurred in obtaining injunctive relief or civil penalties, or both, under this section. Amounts collected by the attorney general under this section shall be deposited in the general revenue fund and may be appropriated only for the investigation and prosecution of other cases under this chapter. A violation of this statute is also a deceptive trade practice under the Texas Deceptive Trade Practices Act.

Utah	
Statute	Utah Code §§ 13-44-101 *et seq.*
Covered Entity	A person who owns or licenses computerized data that includes personal information concerning a Utah resident.
Personal Information Defined	"Personal Information" means 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 date element is unencrypted or not protected by another method that renders the data unreadable or unusable: (i) social security number; (ii) financial account number, or credit or debit card number and any required security code, access code or password that would permit access to the person's account; or (iii) driver license number or state card identification number.
What Triggers Notice Requirement	"Breach of system security" means an unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information. When an entity becomes aware of a breach, it shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused for identity theft or fraud purposes. If an investigation reveals that the misuse of personal information for identity theft or fraud purposes has occurred, or is reasonably likely to occur, the person shall provide notification to each affected Utah resident.
Encryption/Redaction Safe Harbor	Notification is not required if the accessed personal information was encrypted or protected by another method that renders the data unreadable or unusable.
Exemptions from Notification	Notification not required if the misuse of personal information for identity theft or fraud purposes has not occurred, and is not reasonably likely to occur.
Timing of Notification	Notification must be provided in the most expedient time possible without unreasonable delay considering the legitimate investigative needs of law enforcement if notification will impede a criminal investigation, after determining the scope of the breach, and after restoring the reasonable integrity of the system.
Penalties/Private Cause of Action	The statute does not create a private right of action, but also does not affect any private right of action that may exist under other law, including contract or tort. A person who violates this subchapter is subject to a civil penalty:

Utah	
	(i) no greater than $2,500 for a violation or series of violations concerning a specific consumer; and (ii) no greater than $100,000 in the aggregate for related violations concerning more than one consumer unless the violations concern 10,000 or more consumers of Utah and 10,000 or more consumers who are residents of another state. The Attorney General may also seek injunctive relief and attorneys' fees and costs.

Vermont	
Statute	9 V.S.A. §§ 2430, 2435
Covered Entity	Any person who, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates, or otherwise deals with personally identifiable information, and includes the State, State agencies, political subdivisions of the State, public and private universities, privately and publicly held corporations, limited liability companies, financial institutions, and retail operators, that owns or licenses computerized personally identifiable information that includes personal information
Personal Information Defined	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, redacted, or otherwise protected by another method that renders them unreadable or unusable by unauthorized persons: (i) Social Security number; (ii) a 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; (iii) financial account number or credit or debit card number, if the number could be used without additional identifying information, access codes, or passwords; (iv) A password, personal identification number, or other access code for a financial account (v) 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 unique physical representation or digital representation of biometric data; and (vi) Either: (I) health records or records of a wellness program or similar program of health promotion or disease prevention; (II) a health care professional's medical diagnosis or treatment of the consumer; or (III) a health insurance policy number.
What Triggers Notice Requirement	"Security breach" means unauthorized acquisition of electronic data or a reasonable belief of unauthorized acquisition of electronic data that compromises the security, confidentiality, or integrity of a

Vermont

	consumer's personally identifiable information or login credentials maintained by an entity. In determining whether personally identifiable information or login credentials have been acquired or is reasonably believed to have been acquired by a person without valid authorization, an entity may consider the following factors, among others: (i) 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; (ii) indications that the information has been downloaded or copied; (iii) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported; or (iv) that the information has been made public. After discovery or notification of a breach, consumers must be notified.
Encryption/Redaction Safe Harbor	Notification is not required if both the individual's name and the combined data element are encrypted, redacted, or protected by another method that renders them unreadable of unusable.
Exemptions from Notification	Notification is not required if it is established that misuse of the personal information is not reasonably possible and the entity provides notice of the determination that the misuse of the personal information is not reasonably possible to the attorney general or to the Department of Financial Regulation in the event that the data collector is a person or entity licensed or registered with the Department.
Timing of Notification	Notification must be made in the most expedient time possible and without unreasonable delay, but not later than 45 days after the discovery or notification, consistent with the legitimate needs of law enforcement and any measures necessary to determine the scope of the security breach and restore the reasonable integrity, security, and confidentiality of the data system. Notice may be delayed if a law enforcement agency 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. The request for a delay must be made in writing or documented contemporaneously in writing by the entity. If more than 1000 consumers are notified at one time, the entity shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.

Vermont	
	An entity must provide notice of the breach to the Department of Financial Regulation, if regulated by that Department, or to the attorney general. However, 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.
Penalties/Private Cause of Action	The Attorney General and state's attorney shall have sole and full authority to investigate potential violations and to enforce, prosecute, obtain, and impose remedies for any violation.

Virginia	
Statute	Va. Code §§ 18.2-186.6 Va. Code § 32.1– 127.1:05 Va. Code § 58.1-341.2
Covered Entity	**Personal Information Breach Notification Statute**: Natural persons or corporations, business trusts, estates, partnerships, limited partnerships, limited liability partnerships, limited liability companies, associations, organizations, joint ventures, governments, governmental subdivisions, agencies, or instrumentalities or any other legal entity, whether for profit or not for profit **Medical Information Breach Notification Statute**: Any authority, board, bureau, commission, district or agency of the Commonwealth or of any political subdivision of the Commonwealth, including cities, towns and counties, municipal councils, governing bodies of counties, school boards and planning commissions; boards of visitors of public institutions of higher education; and other organizations, corporations, or agencies in the Commonwealth supported wholly or principally by public funds
Personal Information Defined	**Personal Information Breach Notification Statute**: "Personal Information" means 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 Virginia resident, when the data elements are neither encrypted nor redacted: (i) social security number; (ii) driver's license number of state identification card number; (iii) financial account number, credit card 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. (iv) passport number; or (v) military identification number. **Medical Information Breach Notification Statute**: Medical information of Virginia residents. "Medical information" means the first name or first initial and last name with any of the following elements that relate to a resident of the Commonwealth, when the data elements are neither encrypted nor redacted: 1. 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 2. 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

Virginia

	individual's application and claims history, including any appeals records.
What Triggers Notice Requirement	**Personal Information Breach Notification Statute**: "Breach of the security of the system" means the unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes, or it is reasonably believed that it has or will cause, identity theft or other fraud to any Virginia resident. If unencrypted or unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person and causes, or the individual or entity reasonably believes has caused or will cause, identity theft or another fraud to any resident of the Commonwealth, an individual or entity that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach of the security of the system to the attorney general and any affected Virginia resident. **Medical Information Breach Notification Statute**: "Breach of the security of the system" means unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security, confidentiality, or integrity of medical information maintained by an entity. If unencrypted or unredacted medical information was or is reasonably believed to have been accessed and acquired by an unauthorized person, an entity that owns or licenses computerized data that includes medical information shall disclose any breach of the security of the system following discovery or notification of the breach of the security of the system to the Office of the Attorney General, the Commissioner of Health, the subject of the medical information, and any affected resident of the Commonwealth.
Encryption/Redaction Safe Harbor	**Personal Information Breach Notification Statute**: Notification is not required under either statute if the accessed personal information was encrypted or redacted, and there was no access to the encryption key. **Medical Information Breach Notification Statute:** Notification is not required if the information is encrypted, and the encryption key was not compromised, or the information was redacted.
Exemptions from Notification	**Personal Information Breach Notification Statute**: Notification is not required if the entity concludes that there is no reasonable belief that the breach has caused, or will cause, identity theft or another fraud.
Timing of Notification	**Personal Information Breach Notification Statute**: Notification must be made to the attorney general and any affected resident of Virginia without unreasonable delay.

Virginia	
	Notice required by this section may be reasonably delayed to allow the individual or entity to determine the scope of the breach of the security of the system and restore the reasonable integrity of the system. Notice required by this section may be delayed if, after the individual or entity notifies a law enforcement agency, the law enforcement agency determines and advises the individual or entity that the notice will impede a criminal or civil investigation, or homeland or national security. If more than 1000 people are notified at one time, the individual or entity must notify, without unreasonable delay, the attorney general and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis. **Medical Information Breach Notification Statute: The entity must notify the attorney general**, the Commissioner of Health, the subject of the medical information, and any affected resident of the Commonwealth without unreasonable delay. Notice required by this section may be reasonably delayed to allow the entity to determine the scope of the breach of the security of the system and restore the reasonable integrity of the system. 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. If more than 1000 people at notified at one time, the entity shall notify, without unreasonable delay, the attorney general and the Commissioner of Health.
Penalties/Private Cause of Action	**Personal Information Breach Notification Statute**: The Attorney General may bring an action to address violations by imposing 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. Nothing shall limit an individual from recovering direct economic damages from a violation of this law.

Washington	
Statute	Wash. Rev. Code §§ 19.255.010 *et seq.*
Covered Entity	Any person or business that conducts business in this state and that owns or licenses data that includes personal information.
Personal Information Defined	An individual's first name or first initial and last name in combination with any one or more of the following data elements: (i) social security number; (ii) driver's license number or Washington identification card number; (iii) 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; (iv) full date of birth; (v) private key that is unique to an individual and that is used to authenticate or sign an electronic document; (vi) student, military, or passport identification number; (vii) health insurance policy number or health insurance identification number; (viii) 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 (ix) 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. Personal Information also includes any of the data elements described above without the individual's first name or first initial and last name if: (A) encryption, redaction, or other methods have not rendered the data element or combination of data elements unusable; and (B) the data element or combination of data elements would enable a person to commit identity theft against the individual. Personal Information also includes a username or email address in combination with a password or security questions and answers that would permit access to an online account.
What Triggers Notice Requirement	"Breach of the security of the system" means unauthorized acquisition of data the compromises the security, confidentiality, or integrity of personal information. The breach shall be disclosed to residents whose personal information was, or is reasonably believed to have been,

Washington	
	acquired by an unauthorized person and the personal information was not secured.
Encryption/Redaction Safe Harbor	Notification is not required if the accessed personal information was encrypted, unless the confidential process, encryption key, or other means to decipher the secured information was also acquired by an unauthorized person.
Exemptions from Notification	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.
Timing of Notification	Notice must be given to residents in the most expedient time possible and without unreasonable delay, no more than 30 calendar days after the breach was discovered, unless at the request of law enforcement consistent with 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. Notification may be delayed if the entity 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. An entity that is required to notify more than 500 hundred residents as a result of a single breach, must notify the attorney general no more than 30 days after the breach was discovered.
Penalties/Private Cause of Action	The attorney general may enforce this statute. A violation is an unfair deceptive act in trade or commerce and an unfair method of competition. A consumer injured may institute a civil action to recover damages.

West Virginia	
Statute	W. Va. Code §§ 46A-2A-101 *et seq.*
Covered Entity	Individuals or corporations, business trusts, estates, partnerships, limited partnerships, limited liability partnerships, limited liability companies, associations, organizations, joint ventures, governments, governmental subdivisions, agencies or instrumentalities, or any other legal entity, whether for profit or not for profit, that owns or licenses computerized data that includes personal information.
Personal Information Defined	An individual's first name or first initial and last name linked to any one or more of the following data elements that relate to a West Virginia resident, when the data elements are neither encrypted nor redacted (i) social security number; (ii) driver's license number or state identification card number; (iii) financial account number, or credit card, or debit card number in combination with any required security code, access code or password that would permit access to a resident's financial accounts.
What Triggers Notice Requirement	"Breach of the security of a system" means the unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes the individual or entity to reasonably believe that the breach of security has caused or will cause identity theft or other fraud to any resident of West Virginia. The entity must give notice of any breach of the security of a system, following discovery or notification of the breach, to any resident whose unencrypted and unredacted personal information was, or is reasonably believed to have been, accessed and acquired by an unauthorized person and that causes, or it is reasonably believed that it has or will cause, identity theft or other fraud to any West Virginia resident.
Encryption/Redaction Safe Harbor	Notification is not required if the accessed personal information was encrypted or redacted, and there was no access to the encryption key and no reasonable belief that the breach caused or will cause identity theft or other fraud to any resident of West Virginia.
Exemptions from Notification	Notification is required only if the entity reasonably believes the breach has or will cause identity theft or other fraud to any West Virginia resident.
Timing of Notification	Notice must be made without unreasonable delay unless steps are necessary to determine the scope of the breach and to restore the reasonable integrity of the system.

West Virginia	
	Notice 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. If notice to more than 1000 individuals is required, the entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on a nationwide basis.
Penalties/Private Cause of Action	Failure to comply constitutes an unfair or deceptive act of practice, which may be enforced by the Attorney General. The Attorney General shall have exclusive authority to bring an action. No civil penalty may be assessed in an action unless the court finds that the defendant has engaged in a course of repeated and willful violations. No civil penalty shall exceed $150,000 per breach of security of the system or series of breaches of a similar nature that are discovered in a single investigation.

Wisconsin

Statute	Wis. Stat. § 134.98
Covered Entity	An entity whose principal place of business is located in this state or an entity that maintains or licenses personal information in this state, or an entity whose principal place of business is not located in this state knows that personal information pertaining to a resident of this state. An entity means a person, other than an individual, that does any of the following: (i) Conducts business in this state and maintains personal information in the ordinary course of business. (ii) Licenses personal information in this state. (iii) Maintains for a resident of this state a depository account. (iv) Lends money to a resident of this state. "Entity" includes all of the following: (i) The state 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. (ii) A city, village, town, or county.
Personal Information Defined	An individual's last name and the individual's first name or first initial, in combination with and linked to any of the following elements, if the element is not publicly available information and is not encrypted, redacted, or altered in a manner that renders the element unreadable: (i) the individual's Social Security number; (ii) the individual's driver's license number or state identification number; (iii) the number of the individual's financial account number, including a credit or debit card account number, or any security code, access code, or password that would permit access to the individual's financial account; (iv) DNA profile; or (v) the individual's unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation.
What Triggers Notice Requirement	If an entity knows that personal information in its possession has been acquired by an unauthorized person, the entity shall make reasonable efforts to notify each subject of the personal information.

Wisconsin	
Encryption/Redaction Safe Harbor	Notification is not required if one of the data elements linked to an individual's name is encrypted, redacted, or altered in a manner that renders the element unreadable.
Exemptions from Notification	Notification is not required if the acquisition of personal information does not create a material risk of identity theft or fraud to the subject of the personal information.
Timing of Notification	Notice must be provided within a reasonable time, not to exceed **45 days** after the entity learns of the acquisition of personal information. A determination as to reasonableness shall include consideration of the number of notices that an entity must provide and the methods of available communication. Notification may be delayed if a law enforcement agency determines this is necessary to protect an investigation or homeland security. If notification is required for more than 1000 individuals, the entity shall without unreasonable delay notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.
Penalties/Private Cause of Action	Failure to comply with this section is not negligence or a breach of any duty, but may be evidence of negligence or breach of a legal duty.

Wyoming	
Statute	Wyo. Stat. §§ 6-3-901, 40-12-501, 40-12-502
Covered Entity	An individual or commercial entity that conducts business in Wyoming and that owns or licenses computerized data that includes personal identifying information about a resident of Wyoming.
Personal Information Defined	"Personal identifying information", which includes the first name or first initial and last name of a person combined with one or more of the following data elements when either the name or the data elements are unredacted: (i) Address; (ii) Telephone number; (iii) Social Security number; (iv) driver's license number; (v) account number, credit card number or debit card number combined with any security code, access code or password that would allow access to a financial account of the person; (iv) Tribal identification card; (vii) Federal or State government issued identification card; (viii) shared secrets or security tokens that are known to be used for data based authentication; (ix) username or e-mail address combined with a password or security question and answer that would permit access to an online account; (x) birth or marriage certificate; (xi) medical information, meaning a person's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; (xii) 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; (xiii) unique biometric data, meaning data generated from measurements or analysis of human body characteristics for authentication purposes; or (xiv) individual taxpayer identification number.
What Triggers Notice Requirement	"Breach of the security of the data system" means unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal identifying information that causes or it is reasonably believed that it will cause loss or injury to a Wyoming resident. When an individual or entity

Wyoming	
	become aware of a breach it must conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal identifying information has been or will be misused. If the investigation determines that the misuse of personal identifying information about a Wyoming resident has occurred or is reasonably likely to occur, notice must be given as soon as possible to the affected Wyoming resident.
Encryption/Redaction Safe Harbor	Notification is not required if the accessed personal identifying information was redacted.
Exemptions from Notification	Notification is not required if misuse of personal identifying information has not occurred and is not reasonably likely to have occurred.
Timing of Notification	Notification must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.
Penalties/Private Cause of Action	The Attorney General may bring an action in law or equity to address any violation and for other relief that may be appropriate to ensure proper compliance, to recover damages, or both.