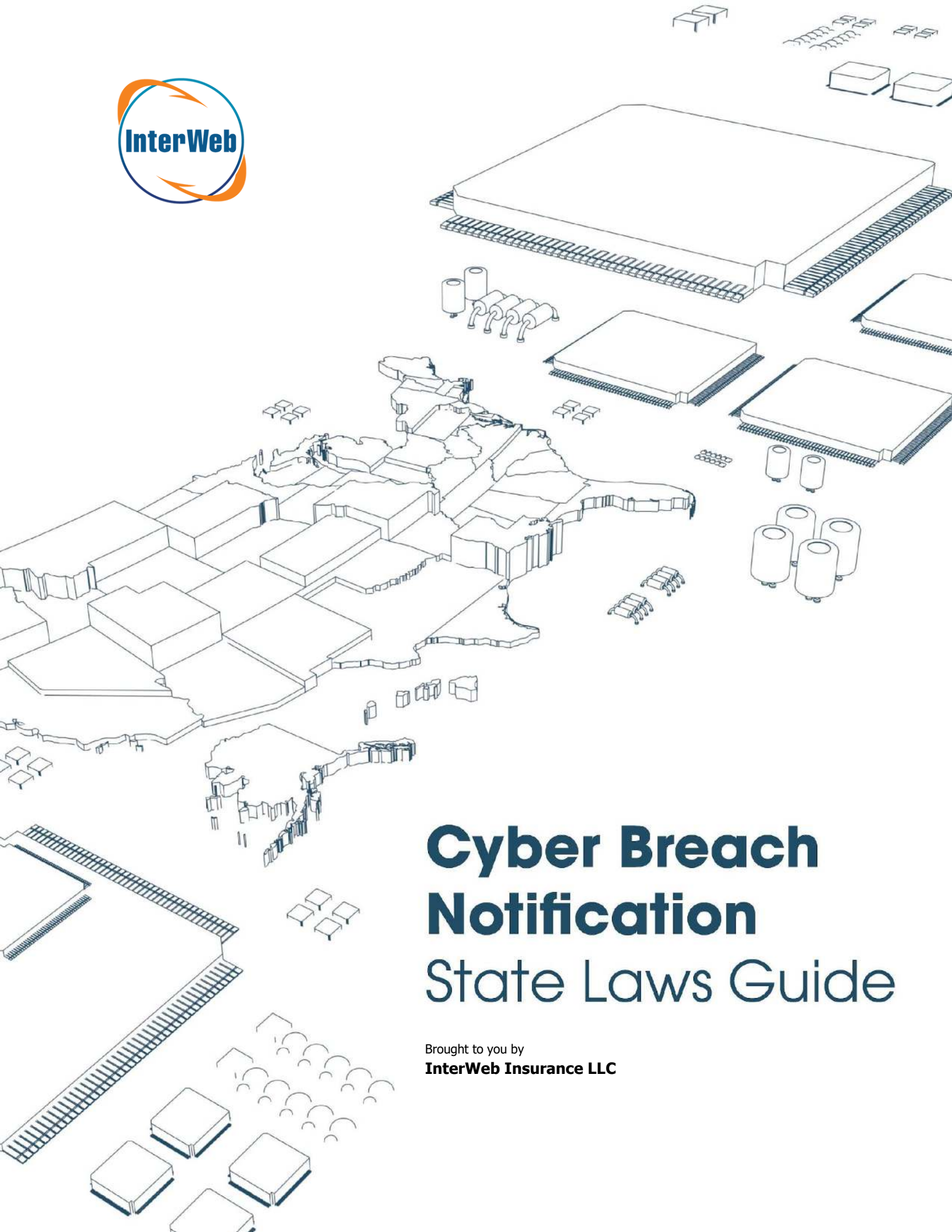

Cyber Breach Notification

State Laws Guide

Brought to you by

InterWeb Insurance LLC

Table of Contents

This guide is for informational purposes only and is intended merely as a high-level overview of state data breach laws. The content below provides a summary of state notification requirements for when an organization's security breach has compromised personal information about the organization's vendors, employees, clients or customers. Data breach events can be dynamic occurrences, and because of this, the regulations that pertain to these circumstances continue to evolve. Organizations that experience a data breach incident are strongly encouraged to use this guide only as a starting point for a multifaceted approach that may include involving their legal counsel.

Importantly, the chart below covers entities that own their data and excludes public entities and non-owners of data. Moreover, this guide presents generally applicable information; it does not introduce or explore the issue of exceptions to the law based on competing compliance requirements, such as the obligations prescribed by the Health Insurance Portability and Accountability Act (HIPAA) or the Gramm-Leach-Bliley Act (GLBA).

Alabama

Statute (link)	Ala. Code 8-38-1 through 8-38-12
What's a breach?	A 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. A breach does not include any of the following: • Good faith acquisition of sensitive personally identifying information by an employee or agent of a covered entity, unless the information is used for a purpose unrelated to the business or subject to further unauthorized use • The release of a public record not otherwise subject to confidentiality or nondisclosure requirements • Any lawful investigative, protective or intelligence activity of a law enforcement or intelligence agency of the state or a political subdivision of the state
What's considered personal information?	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: • A nontruncated Social Security number or tax identification number • A nontruncated 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 • 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 • Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional • An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual • A username or email address in combination with a password or security question and answer that would permit access to an online account affiliated with the covered entity that is

	reasonably likely to contain or is used to obtain sensitive, personally identifying information Personal information does not include: ● Information about an individual that has been lawfully made public by a federal, state or local government record or a widely distributed media; or ● Information that 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.
Individual notification requirements	Notice to individuals must be made as expeditiously as possible and without unreasonable delay, considering the time necessary to allow the covered entity to conduct an investigation. The covered entity must provide notice **within 45 days** of the covered entity's receipt of notice from a third-party agent that a breach has occurred or upon the covered entity's determination that a breach has occurred and is reasonably likely to cause substantial harm to the individuals to whom the information relates. If a federal or state law enforcement agency determines that notice to individuals required would interfere with a criminal investigation or national security, the notice must be delayed upon the receipt of written request of the law enforcement agency for a period that the law enforcement agency determines is necessary. A law enforcement agency, by a subsequent written request, may revoke the delay as of a specified date or extend the period set forth in the original request if further delay is necessary.

Regulator notification requirements	If the number of individuals a covered entity is required to notify **exceeds 1,000**, the entity must provide written notice of the breach to the state attorney general as expeditiously as possible and without unreasonable delay. The covered entity must provide the notice **within 45 days** of the covered entity's receipt of notice from a third-party agent that a breach has occurred or upon the entity's determination that a breach has occurred and is reasonably likely to cause substantial harm to the individuals to whom the information relates.
Enforcement	Any covered entity that is knowingly engaging in or has knowingly engaged in a violation of the notification provisions is subject to penalty provisions. Knowingly must mean willfully or with reckless disregard in failing to comply with notice requirement. Civil penalties assessed will not exceed $500,000 per breach. A covered entity that violates the notification provisions will be liable for a civil penalty of not more than $5,000 per day for each consecutive day that the covered entity fails to take reasonable action to comply with the notice provisions.

Alaska

Statute (link)	AK 45.48.010-.090
What's a breach?	Breach of security means the 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: • A photocopy, facsimile or another paper-based method; • A device, including a computer, that can read, write or store information that is represented in numerical form; or • A method not identified above.

What's considered personal information?	Information in any form on an individual that is not encrypted or redacted (or is encrypted and the encryption key has been accessed or acquired) and consists of a combination of an individual's:
	• First name or initial;
	• Last name; and
	• One or more of the following information elements for the individual:
	  ○ Social security number;
	  ○ Driver's license number or state identification card number;
	  ○ Account number, credit card number or debit card number; or
	  ○ The security code, access code, personal identification number or password (if required to access account or card mentioned above).

Individual notification requirements	If a covered entity owns or licenses personal information in any form that includes personal information on a state resident and a breach of the security of the information system that contains personal information occurs, the covered entity must, after discovering or being notified of the breach, disclose the breach to each state resident whose personal information was subject to the breach. An information collector must make the disclosure mentioned above in the most expeditious time possible and without unreasonable delay, except if there is an allowable delay in notification and as necessary to determine the scope of the breach and restore the reasonable integrity of the information system.
Regulator notification requirements	If an information collector is required to disclose the breach to notify **more than 1,000** state residents of a breach, the information collector must also notify, without unreasonable delay, all consumer credit reporting agencies that compile and maintain files on consumers

	on a nationwide basis and provide the agencies with the timing, distribution and content of the notices to state residents.
Enforcement	The violation of a state resident's personal information standards is an unfair or deceptive act or practice if: • The information collector is not a governmental agency; and • The violation takes place in the conduct of trade or commerce. Information collectors are not subject to civil penalties imposed under the unfair trade practices and consumer protection but are liable to the state for a civil penalty of up to $500 and damages for each state resident who was not notified under this standard. However, the total civil penalty may not exceed $50,000, and damages are limited to actual economic damages that do not exceed $500.

Arizona

Statute (link)	Ariz. Rev. Stat. § 44-7501
What's a breach?	A breach means 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 individuals. A breach does not include a good faith acquisition of personal information by a person's employee or agent for the purposes of the person if the personal information is not used for a purpose unrelated to the person and is not subject to further unauthorized disclosure.
What's considered personal information?	Personal information means any of the following: • An individual's first name or first initial and last name in combination with one or more specified data elements; or • An individual's username or email address in combination with a password or security question and answer that allows access to an online account. Personal information does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media.
Individual notification requirements	If the investigation results in a determination that there has been a security system breach, the person who owns or licenses the computerized data must notify the individuals affected **within 45 days** after the determination. Notifications may be delayed if a law enforcement agency advises the person who the notifications will impede a criminal investigation. When the law enforcement agency determines the notifications no longer would compromise the investigation, notifications are required to be made **within 45 days**.
Regulator notification requirements	If the breach requires notification of **more than 1,000 individuals**, notify both: • The three largest nationwide consumer reporting agencies; and • The attorney general, in writing, in a form prescribed by rule or order of the attorney general or by providing the attorney general with a copy of the notification provided.
Enforcement	A knowing and willful violation is an unlawful practice, and only the attorney general may enforce such a violation by investigating and taking appropriate action. The attorney general may impose a civil penalty for a violation not to exceed the lesser of $10,000 per affected individual or the total amount of economic loss sustained by affected individuals, but the maximum civil penalty from a breach or series of

	related breaches may not exceed $500,000. The attorney general can still recover restitution for affected individuals.

Arkansas

Statute (link)	**Ark. Code § 4-110-101 et seq.**
What's a breach?	A breach is the unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal information maintained by a person or business. A breach does not include the good faith acquisition of personal information by an employee or agent of the person or business for the legitimate purposes of the person or business if the personal information is not otherwise used or subject to further unauthorized disclosure.

What's considered personal information?	Personal information means an individual's:
	• First name or first initial;
	• Last name; and
	• One or more of the following information elements for the individual:
	  ○ Social security number;
	  ○ Driver's license number or Arkansas identification card number;
	  ○ Account number, credit card number or debit card number;
	  ○ The security code, access code, personal identification number or password (if required to access account or card mentioned above); or
	• Medical information; and
	• Biometric data: data generated by automatic measurements of an individual's biological characteristics, including, without limitation:
	  ○ Fingerprints;
	  ○ Faceprint;
	  ○ A retinal or iris scan;
	  ○ Hand geometry;
	  ○ Voiceprint analysis;
	  ○ Deoxyribonucleic acid (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.

Individual notification requirements	Any person or business that acquires, owns or licenses computerized data that includes personal information must disclose any breach of the security of the system following discovery or notification of the breach of the security of the system to any resident of Arkansas whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person.

	The disclosure must be made in the most expedient time and manner 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 reasonable integrity of the data system. Notification can be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. Notification must be made after the law enforcement agency determines that it will not compromise the investigation.
Regulator notification requirements	If a breach of the security of a system affects the personal information of **more than 1,000 individuals**, the person or business required to make a disclosure of the security breach must, at the same time the security breach is disclosed to an affected individual or **within 45 days** after the person or business determines that there is a reasonable likelihood of harm to customers, whichever occurs first, disclose the security breach to the attorney general.
Enforcement	Any violation of this chapter is punishable by action of the attorney general. Any person who knowingly and willfully commits an unlawful practice under this chapter will be guilty of a Class A misdemeanor.

California

Statute (link)	**Cal. Civ. Code § 1798.29; 1798.82 et seq.**
What's a breach?	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 agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.
What's considered personal information?	Personal information means an individual's first name or first initial and last name in combination with one or more of the following data elements when either the name or the data elements are not encrypted: • Social security number; • 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; • 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; • Medical information; • Health insurance information; • 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. Unique biometric data does not include a physical or digital photograph unless used or stored for facial recognition purposes; or • Information or data collected through the use or operation of an automated license plate recognition system. Personal information does not include publicly available information that is lawfully made available to the general public from federal, state or local government records.
Individual notification requirements	Any agency that owns or licenses computerized data that includes personal information must disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose: • Unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person or • 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 agency that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that personal information readable or usable. The disclosure 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.
Regulator notification requirements	Any agency that is required to issue a security breach notification to **more than 500 California residents** as a result of a single breach of the security system must electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the attorney general. A single sample copy of a security breach notification must not be deemed to be within the Inspection of Public Records of the Government Code.
Enforcement	Any person other than an employee of the state or of a local government agency acting solely in his or her official capacity who intentionally discloses information not otherwise public, which they know or should reasonably know was obtained from personal information maintained by a state agency or from "records" within a "system of records," is subject to a civil action, for invasion of privacy, by the individual to whom the information pertains. In any successful action brought, the complainant, in addition to any special or general damages awarded, must be awarded a minimum of $2,500 in exemplary damages as well as attorney's fees and other litigation costs reasonably incurred in the suit. The right, remedy and cause of action must be nonexclusive and is in addition to all other rights, remedies and causes of action for invasion of privacy inherent in Section 1 of Article I of the California Constitution.

Colorado

Statute (link)	Colo. Rev. Stat. § 6-1-716
What's a Breach?	A breach consists of the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality or integrity of personal information maintained by an individual or a commercial entity. Good faith acquisition of personal information by an employee or agent of an individual or commercial entity for the purposes of the individual or commercial entity is not a breach of the security of the system if the personal information is not used for (or is not subject to) further unauthorized disclosure.
What's considered personal information?	Personal information includes a Colorado resident's first name or first initial and last name in combination with one or more of the following data elements that relate to the resident when the data elements are not encrypted, redacted or secured by any other method rendering the name or the element unreadable or unusable: • Social security number; • Student, military or passport identification number; • Driver's license number or identification card number; • Medical information; • Health insurance identification number; • Biometric data; • Username or email address, in combination with a password or security questions and answers, that would permit access to an online account; 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 that account. Personal information does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media.
Individual notification requirements	The covered entity must give notice to affected Colorado residents unless the investigation determines that the misuse of information about a Colorado resident has not occurred and is not reasonably likely to occur. Notice must be made in the most expedient time possible and without unreasonable delay, but not later than **30 days** after the date of determination that a security breach occurred, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system. A required notice may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation and the law enforcement agency has notified the individual or commercial entity that conducts business in Colorado not to send required notices.

	The required notice must be made in good faith, without unreasonable delay and as soon as possible after the law enforcement agency determines that notification will no longer impede the investigation and has notified the individual or commercial entity that conducts business in Colorado that it is appropriate to send the required notice.
Regulator notification requirements	The covered entity that must notify Colorado residents of a data breach must provide notice of any security breach to the Colorado attorney general in the most expedient time possible and without unreasonable delay but no later than **30 days** after the date of determination that a security breach occurred if the security breach is reasonably believed to have affected **500 Colorado residents or more** unless the investigation determines that the misuse of information about a Colorado resident has not occurred and is not likely to occur. If a covered entity is required to notify **more than 1,000 Colorado residents** of a security breach, the covered entity must also notify, in the most expedient time possible and without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by the federal "Fair Credit Reporting Act," 15 U.S.C. sec. 1681a (p), of the anticipated date of the notification to the residents and the approximate number of residents who are to be notified. The covered entity is not required to provide the consumer reporting agency with the names or other personal information of security breach notice recipients.
Enforcement	The attorney general may bring an action in law or equity to address violations and for other relief that may be appropriate to ensure compliance with this data breach notification requirements or to recover direct economic damages resulting from a violation or both. These provisions are not exclusive and do not relieve a covered entity from compliance with all other applicable provisions of law. Upon receipt of notice and with either a request from the governor to prosecute a particular case or approval of the district attorney with jurisdiction to prosecute cases in the judicial district where a case could be brought, the attorney general has the authority to prosecute any criminal violations of section 18-5.5-102.

Connecticut

Statute (link)	Conn. Gen. Stat. § 36a-701b
What's a breach?	A breach of security means unauthorized access to or unauthorized acquisition of electronic files, media, databases or computerized data containing 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.
What's considered personal information?	Personal information means an individual's first name or first initial and last name in combination with one or more of the following data: • Social Security number; • Driver's license number or state identification card number; • Credit or debit card number; or • Financial account number in combination with any required security code, access code or password that would permit access to such financial account. Personal information does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media.
Individual notification requirements	Notice of breach must be made without unreasonable delay but not later than **90 days** after the discovery of such breach unless a shorter time is required under federal law and the completion of an investigation by such person to determine the nature and scope of the incident, to identify the individuals affected or to restore the reasonable integrity of the data system. However, notification is not required if, after an appropriate investigation and consultation with relevant federal, state and local agencies responsible for law enforcement, the person reasonably determines that the breach will not likely result in harm to the individuals whose personal information has been acquired and accessed. Any required notification must be delayed for a reasonable period of time if a law enforcement agency determines that the notification will impede a criminal investigation and such law enforcement agency has made a request for the notification to be delayed. Any such delayed notification must be made after such law enforcement agency determines that notification will not compromise the criminal investigation and so notifies the person of such determination.
Regulator notification requirements	The 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, must, not later than the time when notice is provided to the resident, also provide notice of the breach of security to the attorney general.
Enforcement	Failure to comply with data breach notification requirements constitutes an unfair trade practice and must be enforced by the attorney general.

Delaware

Statute (link)	Del. Code Ann. tit. 6 § 12B-101 et seq.
What's a breach?	A breach is the unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal information. Good faith acquisition of personal information by an employee or agent of any person for the purposes of such person is not a breach of security, provided that the personal information is not used for an unauthorized purpose or subject to further unauthorized disclosure. The unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal information is not a breach of security to the extent that personal information contained therein is encrypted unless such unauthorized acquisition includes or is reasonably believed to include the encryption key and the person who owns or licenses the encrypted information has a reasonable belief that the encryption key could render that personal information readable or useable.
What's considered personal information?	Personal information means a Delaware resident's first name or first initial and last name in combination with one or more of the following data elements that relate to that individual: • Social Security number; • Driver's license number or state or federal identification card number; • Account number, credit card number or debit card number, in combination with any required security code, access code or password that would permit access to a resident's financial account; • Passport number; • A username or email address, in combination with a password or security question and answer that would permit access to an online account; • Medical history, medical treatment by a health care professional, diagnosis of mental or physical condition by a health care professional or DNA profile; • Health insurance policy number, subscriber identification number or any other unique identifier used by a health insurer to identify the person; • Unique biometric data generated from measurements or analysis of human body characteristics for authentication purposes; or • An individual taxpayer identification number.

	Personal information does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media.
Individual notification requirements	A person who conducts business in the state and owns or licenses computerized data that includes personal information must provide notice without unreasonable delay but no later than **60 days** after the determination of the breach of security. However, this is not required if: ● A shorter time is required under federal law; ● A law enforcement agency determines that the notice will impede a criminal investigation, and such law enforcement agency has made a request of the person that the notice be delayed. Any delayed notice must be made after such law enforcement agency determines that the notice will not compromise the criminal investigation and so notifies the person of such determination; or ● When a person 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 the 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.
Regulator notification requirements	If the affected number of Delaware residents to be notified **exceeds 500 residents**, the person required to provide notice must not do so later than the time when notice is provided to the resident and also provide notice of the breach of security to the attorney general.
Enforcement	The attorney general may bring an action in law or equity to address violations and for other relief that may be appropriate to ensure proper compliance or to recover direct economic damages resulting from a violation or both. The provisions of this chapter are not exclusive and do not relieve a person subject to this chapter from compliance with all other applicable provisions of law.

District of Columbia

Statute (link)	D.C. Code § 28-3851 et seq.
What's a breach?	A breach is an unauthorized acquisition of computerized or other electronic data or any equipment or device storing such data that compromises the security, confidentiality or integrity of personal information maintained by the person or entity that conducts business in the District of Columbia. Data breach **does not** include: • A good faith acquisition of personal information by an employee or agency of the person or entity for the purposes of the person or entity if the personal information is not used improperly or subject to further unauthorized disclosure; • Acquisition of data that has been rendered secure, including through encryption or redaction of such data, to be unusable by an unauthorized third party unless any information obtained has the potential to compromise the effectiveness of the security protection preventing unauthorized access; or • Acquisition of personal information of an individual that the person or entity reasonably determines, after a reasonable investigation and consultation with the Office of the Attorney General for the District of Columbia and federal law enforcement agencies, will likely not result in harm to the individual.
What's considered personal information?	Personal information includes an individual's first name, first initial and last name or any other personal identifier, which, in combination with any of the following data elements, can be used to identify a person or the person's information: • Social security number, Individual Taxpayer Identification Number, passport number, driver's license number, District of Columbia identification card number, military identification number or other unique identification number issued on a government document commonly used to verify the identity of a specific individual; • Account number, credit card number or debit card number or any other number or code or combination of numbers or codes, such as an identification number, security code, access code or password, that allows access to or use of an individual's financial or credit account; • Medical information; • Genetic information and DNA profile; • Health insurance information, including a policy number, subscriber information number or any unique identifier used by

	a health insurer to identify the person who permits access to an individual's health and billing information; • Biometric data of an individual generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, genetic print, retina or iris image or other unique biological characteristics, that is used to uniquely authenticate the individual's identity when the individual accesses a system or account; • Any combination of data elements previously mentioned that would enable a person to commit identity theft without reference to a person's first name or first initial and last name or another independent personal identifier; or • A username or email address in combination with a password, security question and answer or other means of authentication or any combination of data elements included in the list above that permits access to an individual's email account.
Individual notification requirements	Any person or entity that 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 and who discovers a breach of the security of the system must promptly notify any District of Columbia resident whose personal information was included in the breach. The notification must be made 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 data system.
Regulator notification requirements	In addition to giving the notification promptly without unreasonable delay and consistent with the legitimate needs of law enforcement, the person or entity required to give notice must promptly provide written notice of the breach of the security of the system to the Office of the Attorney General for the District of Columbia if the breach affects **50 or more** District of Columbia residents. This notice must be made in the most expedient manner possible, without unreasonable delay and in no event later than when notice is provided to District of Columbia residents. This notice must not be delayed on the grounds that the total number of District of Columbia residents affected by the breach has not yet been ascertained. If any person or entity is required to notify **more than 1,000 persons** of a breach of security, the person must also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution and content of the notices.
Enforcement	A violation of the requirements is an unfair or deceptive trade practice. The rights and remedies available for data breach notification

	violations are cumulative to each other and any other rights and remedies available under law.

Florida

Statute (link)	Fla. Stat. § 501.171
What's a breach?	A breach of security or breach means unauthorized access of data in electronic form containing personal information. Good faith access of personal information by an employee or agent of the covered entity does not constitute a breach of security, provided that the information is not used for a purpose unrelated to the business or subject to further unauthorized use.
What's considered personal information?	Personal information means an individual's first name or first initial and last name in combination with one or more of the following data elements for that individual: • A Social Security number; • A driver's license or identification card number, passport number, military identification number or other similar number issued on a government document used to verify identity; • A financial account number or credit or debit card number, in combination with any required security code, access code or password that is necessary to permit access to an individual's financial account; • Any information regarding an individual's medical history, mental or physical condition or medical treatment or diagnosis by a health care professional; • An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual; or • A username or email address in combination with a password or security question and answer that would permit access to an online account. Personal information does not include information about an individual that has been made publicly available by a federal, state or local governmental entity. The term also does not include information that is encrypted, secured or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable.
Individual notification requirements	A covered entity must give notice to each individual in this state whose personal information was or the covered entity reasonably believes to have been accessed as a result of the breach. Notice to individuals must be made as expeditiously as practicable and without unreasonable delay, taking into account the time necessary to allow the covered entity to determine the scope of the breach of security, to identify individuals affected by the breach and to restore the reasonable integrity of the data system that was breached but no later than **30 days** after the determination of a breach or reason to believe

	a breach occurred unless subject to a delay authorized under 501.171 4(b) or waiver under 501.171 4(c). If a federal, state or local law enforcement agency determines that notice to individuals would interfere with a criminal investigation, the notice must be delayed upon the written request of the law enforcement agency for a specified period that the law enforcement agency determines is reasonably necessary. A law enforcement agency may, by a subsequent written request, revoke such delay as of a specified date or extend the period set forth in the original request made under this paragraph to a specified date if further delay is necessary.
Regulator notification requirements	A covered entity must provide notice to the department of legal affairs of any breach of security affecting 500 or more individuals in this state. Such notice must be provided to the department as expeditiously as practicable, but no later than **30 days** after the determination of the breach or reason to believe a breach occurred. A covered entity may receive 15 additional days to provide notice if a good cause for delay is provided in writing to the department within 30 days after the determination of the breach or reason to believe a breach occurred. If a covered entity discovers circumstances requiring notice of **more than 1,000 individuals** at a single time, the covered entity must also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in the Fair Credit Reporting Act, 15 U.S.C. s. 1681a(p), of the timing, distribution and content of the notices.
Enforcement	A violation of data breach notification requirements is treated as an unfair or deceptive trade practice in any action brought by the department under remedies of enforcing authority (FL Stat. § 501.207) against a covered entity or third-party agent. In addition to the remedies provided for, a covered entity that violates the notice to the department of legal affairs or to individuals is liable for a civil penalty not to exceed $500,000, as follows: • In the amount of $1,000 for each day up to the first 30 days following any violation of notice and $50,000 thereafter for each subsequent 30-day period or portion thereof for up to 180 days; or • In an amount not to exceed $500,000 if the violation continues for more than 180 days. The civil penalties for failure to notify provided apply per breach and not per individual affected by the breach.

Georgia

Statute (link)	Ga. Code § 10-1-910 et seq.
What's a breach?	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 of such individual maintained by an information broker or data collector. Good faith acquisition or use of personal information by an employee or agent of an information broker or data collector for the purposes of such information broker or data collector is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.
What's considered personal information?	Personal information means an individual's first name or first initial and last name in combination with one or more of the following data elements when either the name or the data elements are not encrypted or redacted: • Social Security number; • Driver's license number or state identification card number; • Account number, credit card number or debit card number, if circumstances exist wherein such a number could be used without additional identifying information, access codes or passwords; • Account passwords or personal identification numbers or other access codes; or • Any of the items previously mentioned 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. Personal information does not include publicly available information that is lawfully made available to the general public from federal, state or local government records.
Individual notification requirements	Any information broker or data collector that maintains computerized data including personal information of individuals must give notice of any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. The notice 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, security and confidentiality of the data system.

	Required notification may be delayed if a law enforcement agency determines that the notification will compromise a criminal investigation. The required notification must be made after the law enforcement agency determines that it will not compromise the investigation.
Regulator notification requirements	In the event that an information broker or data collector discovers circumstances requiring notification of **more than 10,000 residents** of this state at one time, the information broker or data collector must also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by 15 U.S.C. Section 1681a, of the timing, distribution and content of the notices.
Enforcement	*Specific enforcement information is not available at this time.*

Hawaii

Statute (link)	Haw. Rev. Stat. § 487N-1 et seq.
What's a breach?	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 creates a risk of harm to a person. Any incident of unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential process or key constitutes a security breach. Good faith acquisition of personal information by an employee or agent of the business for a legitimate purpose is not a security breach, provided that the personal information is not used for a purpose other than a lawful purpose of the business and is not subject to further unauthorized disclosure.
What's considered personal information?	Personal information means an individual's first name or first initial and last name in combination with one or more of the following data elements when either the name or the data elements are not encrypted: • Social Security number; • Driver's license number or Hawaii identification card number; or • Account number, credit or debit card number, access code or password that would permit access to an individual's financial account. Personal information does not include publicly available information that is lawfully made available to the general public from federal, state or local government records.
Individual notification requirements	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 must provide notice to the affected person who there has been a security breach following discovery or notification of the breach. The disclosure notification must be made without unreasonable delay, consistent with the legitimate needs of law enforcement as required by law 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. Required notice must be delayed if a law enforcement agency informs the business or government agency that the notification may impede a criminal investigation or jeopardize national security and requests a delay, provided that such request is made in writing or the business or government agency documents the request contemporaneously in writing, including the name of the law enforcement officer making the

	request and the officer's law enforcement agency engaged in the investigation. The required notice must be provided without unreasonable delay after the law enforcement agency communicates to the business or government agency its determination that notice will no longer impede the investigation or jeopardize national security.
Regulator notification requirements	In the event a business provides notice to **more than 1,000 persons** at one time, the business must 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 consumers on a nationwide basis, as defined in 15 U.S.C. section 1681a(p), of the timing, distribution and content of the notice.
Enforcement	Any business that violates any provision of this chapter is 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. No such action may be brought against a government agency. In addition to previously mentioned penalties, a business that violates any provision of this chapter may be liable to the injured party in an amount equal to the sum of any actual damages sustained by the injured party as a result of the violation. Courts may award reasonable attorneys' fees to the prevailing party in a lawsuit. No such action may be brought against a government agency. These penalties are cumulative to the remedies or penalties available under all other laws of this state.

Idaho

Statute (link)	Idaho Code § 28-51-104 et seq.
What's a breach?	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 maintained by an agency, individual or a commercial entity. Good faith acquisition of personal information by an employee or agent of an agency, individual or a commercial entity for the purposes of the agency, individual or the commercial entity is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.
What's considered personal information?	Personal information means an Idaho resident's first name or first initial and last name in combination with one or more of the following data elements that relate to the resident when either the name or the data elements are not encrypted: • Social Security number; • Driver's license number or Idaho identification card 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 a resident's financial account. Personal information does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media.
Individual notification requirements	If the investigation determines that the misuse of information about an Idaho resident has occurred or is reasonably likely to occur, the agency, individual or the commercial entity must give notice as soon as possible to the affected Idaho resident. 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, to identify the individuals affected and to restore the reasonable integrity of the computerized data system. Required notice may be delayed if a law enforcement agency advises the agency, individual or commercial entity that the notice will impede a criminal investigation. Required notice must be made in good faith, without unreasonable delay and as soon as possible after the law enforcement agency advises the agency, individual or commercial entity that notification will no longer impede the investigation.
Regulator notification requirements	When an agency becomes aware of a breach of the security of the system, it must notify the office of the Idaho attorney general **within 24 hours of the discovery**. Nothing contained in this section relieves a state agency's responsibility to report a security breach to the office of the chief information officer within the department of administration, pursuant to the Idaho technology authority policies.

Enforcement	In any case in which an agency's, commercial entity's or individual's primary regulator has reason to believe that an agency, individual or commercial entity subject to that primary regulator's jurisdiction under section 28-51-104(6), Idaho Code, has violated section 28-51-105, Idaho Code, by failing to give notice in accordance with that section, the primary regulator may bring a civil action to enforce compliance with that section and enjoin that agency, individual or commercial entity from further violations. Any agency, individual or commercial entity that intentionally fails to give notice in accordance with section 28-51-105, Idaho Code, must be subject to a fine of not more than $25,000 per breach of the security of the system.

Illinois

Statute (link)	**815 Ill. Comp. Stat. 530/5, 530/10, 530/12, 530/15, 530/20, 530/25**
What's a breach?	Breach of the security of the system data, or "breach," means unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal information maintained by the data collector. A breach does not include good faith acquisition of personal information by an employee or agent of the data collector for a legitimate purpose of the data collector, provided that the personal information is not used for a purpose unrelated to the data collector's business or subject to further unauthorized disclosure.
What's considered personal information?	Personal information means an individual's first name or first initial and last name in combination with one or more of the following data elements when either the name or the data elements are not encrypted or redacted or are encrypted or redacted, but the keys to unencrypt, unredact or otherwise read the name or data elements have been acquired without authorization through the breach of security: • Social Security number; • Driver's license number or state identification card number; • 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; • Medical information; • Health insurance information; or • Unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee to authenticate an individual, such as a fingerprint, retina or iris image or other unique physical representation or digital representation of biometric data.
Individual notification requirements	Any data collector that owns or licenses personal information concerning an Illinois resident must notify the resident at no charge that there has been a breach following discovery or notification of the breach. The disclosure 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 restore the reasonable integrity, security and confidentiality of the data system. The notification to an Illinois resident may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the data collector with a written request for the delay. However, the data collector must notify the

	Illinois resident as soon as notification no longer interferes with the investigation.
regulator notification Requirements	Any data collector required to issue notice to **more than 500** Illinois residents as a result of a single breach of the security system must provide notice to the attorney general of the breach. The notification must be made in the most expedient time possible and without unreasonable delay but in no event later than when the data collector provides notice to consumers. If the date of the breach is unknown at the time the notice is sent to the attorney general, the data collector must send the attorney general the date of the breach as soon as possible.
Enforcement	A violation of this Act constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act.

Indiana

Statute (link)	**Ind. Code § 4-1-11 et seq.; § 24-4.9-1 et seq.**
What's a breach?	Breach of the security of data means unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal information maintained by a person. 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.

What's considered personal information?	Personal information means:
	• A Social Security number that is not encrypted or redacted; or
	• An individual's first and last names or first initial and last name and one or more of the following data elements that are not encrypted or redacted:
	  ○ A driver's license number;
	  ○ A state identification card number;
	  ○ A credit card number; or
	• A financial account number or debit card number in combination with a security code, password or access code that would permit access to the person's account.
	
	Personal information does not include information that is lawfully obtained from publicly available information or from federal, state or local government records lawfully made available to the general public.

Individual notification requirements	After discovering or being notified of a breach of the security of data, the database owner must disclose the breach to an Indiana resident whose: • Unencrypted personal information was or may have been acquired by an unauthorized person; or • Encrypted personal information was or may have been acquired by an unauthorized person with access to the encryption key. If the database owner knows, should know or should have known that the unauthorized acquisition constituting the breach has resulted in or could result in identity deception (as defined in IC 35-43-5-3.5), identity theft or fraud affecting the Indiana resident. Delay in notification is reasonable when it is necessary to restore the integrity of the computer system or discover the scope of the breach or in response to a request from the attorney general or a law enforcement agency. Once the delay is no longer necessary for the restoration of the system or scope of the breach, notification should be made as soon as possible. Once the attorney general or law enforcement agency notifies the person who the delay no longer impedes a criminal or civil

	investigation or jeopardizes national security, a person must provide notification as soon as possible.
Regulator notification requirements	A database owner required to make a disclosure to **more than 1,000 consumers** must also disclose to each consumer reporting agency (as defined in 15 U.S.C. 1681a(p)) information necessary to assist the consumer reporting agency in preventing fraud, including personal information of an Indiana resident affected by the breach of the security of a system. If a database owner makes a disclosure described above, the database owner must also disclose the breach to the attorney general.
Enforcement	A person who is required to make a disclosure or notification in accordance with IC 24-4.9-3 and fails to comply with any provision of this article commits a deceptive act that is actionable only by the attorney general under this chapter. Each failure to make a required disclosure or notification in connection with a related series of breaches of the security of data constitutes one deceptive act. The attorney general may bring an action to obtain any or all of the following: ● An injunction to enjoin future violations of IC 24-4.9-3. ● A civil penalty of not more than $150,000 per deceptive act. ● The attorney general's reasonable costs in: ● The investigation of the deceptive act; and ● Maintaining the action.

Iowa

Statute (link)	Iowa Code § 715C.1-2
What's a breach?	Breach of security means unauthorized acquisition of personal information maintained in computerized form by a person who compromises the security, confidentiality or integrity of the personal information. Good faith acquisition of personal information by a person or that person's employee or agent for a legitimate purpose of that person is not a breach of security, provided that the personal information is not used in violation of applicable law or in a manner that harms or poses an actual threat to the security, confidentiality or integrity of the personal information.
What's considered personal Information?	Personal information means 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 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: • Social Security number; • Driver's license number or other unique identification number created or collected by a government body; • 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; • 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; • Unique biometric data, such as a fingerprint, retina or iris image or other unique physical representation or digital representation of biometric data. Personal information does not include information that is lawfully obtained from publicly available sources or from federal, state or local government records lawfully made available to the general public
Individual notification requirements	Any person who owns or licenses computerized data that includes a consumer's personal information used in the course of the person's business, vocation, occupation or volunteer activities and that was subject to a breach of security must give notice of the breach of security following discovery of such breach of security or receipt of notification (as required by law) to any consumer whose personal information was included in the information that was breached. The consumer notification must be made in the most expeditious manner possible and without unreasonable delay, consistent with the legitimate needs of law enforcement as required by law and any

	measures necessary to sufficiently determine contact information for the affected consumers, determine the scope of the breach and restore the reasonable integrity, security and confidentiality of the data. Any person who maintains or otherwise possesses personal information on behalf of another person must notify the owner or licensor of the information of any breach of security immediately following discovery of such breach of security if a consumer's personal information was included in the information that was breached. Consumer notification requirements may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation and the agency has made a written request that the notification be delayed. Required notification must be made after the law enforcement agency determines that the notification will not compromise the investigation and notifies the person required to give notice in writing.
Regulator notification requirements	If an entity that owns or licenses computerized data that includes a consumer's personal information used in the course of the entity's business, vocation, occupation or volunteer activities suffers a security breach requiring notification of more than 500 Iowa residents, then the entity will give written notice following discovery of such breach or receipt of notification required by third parties, to the director of the consumer protection division of the attorney general's office. Notice or receipt of notice must be provided **within five business days** of giving notice to any consumer.
Enforcement	A violation of this chapter is an unlawful practice pursuant to section 714.16 and, in addition to the remedies provided to the attorney general pursuant to section 714.16, subsection 7, the attorney general may seek and obtain an order that a party held to violate this section pay damages to the attorney general on behalf of a person injured by the violation.

Kansas

Statute (link)	Kan. Stat. § 50-7a01 et seq.
What's a breach?	Security breach means the unauthorized access and acquisition of unencrypted or unredacted computerized data that compromises the security, confidentiality or integrity of personal information maintained by an individual or a commercial entity and that causes or such individual or entity reasonably believes has caused or will cause identity theft to any consumer. Good faith acquisition of personal information by an employee or agent of an individual or a commercial entity for the purposes of the individual or the commercial entity is not a breach of the security of the system, provided that the personal information is not used for or is not subject to further unauthorized disclosure.
What's considered personal information?	Personal information means a consumer's first name or first initial and last name linked to one or more of the following data elements that relate to the consumer when the data elements are neither encrypted nor redacted: • Social Security number; • Driver's license number or state identification card number; or • 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. Personal information does not include publicly available information that is lawfully made available to the general public from federal, state or local government records.
Individual notification requirements	A person who conducts business in this state or a government, governmental subdivision or agency that owns or licenses computerized data that includes personal information must, when it becomes aware of any breach of the security of the system, 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 information has occurred or is reasonably likely to occur, the person or government, governmental subdivision or agency must give notice as soon as possible to the affected Kansas residents. Notice must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system. Required notice may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation. Required notice must be made in good faith, without unreasonable

	delay and as soon as possible after the law enforcement agency determines that notification will no longer impede the investigation.
Regulator notification requirements	In the event that a person discovers circumstances requiring notification of **more than 1,000 consumers** at one time, the person must also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by 15 U.S.C. § 1681a(p), of the timing, distribution and content of the notices.
Enforcement	For entities other than insurance companies, the attorney general is empowered to bring an action in law or equity to address data breach notification requirement violations and for other relief that may be appropriate. These provisions are not exclusive and do not relieve an individual or a commercial entity subject to these data breach notification requirements from compliance with all other applicable provisions of law.

Kentucky

Statute (link)	KY Rev. Stat. §365.732
What's a breach?	Breach of the security of the system means the unauthorized acquisition of unencrypted and unredacted computerized data that compromises the security, confidentiality or integrity of personally identifiable information maintained by the information holder as part of a database regarding multiple individuals that actually causes or leads the information holder to reasonably believe has caused or will cause, identity theft or fraud against any resident of the Commonwealth of Kentucky. Good faith acquisition of personally identifiable information by an employee or agent of the information holder for the purposes of the information holder is not a breach of the security of the system if the personally identifiable information is not used or subject to further unauthorized disclosure.
What's considered personal information?	Personally identifiable information means an individual's first name or first initial and last name in combination with one or more of the following data elements when the name or data element is not redacted: • Social Security number; • Driver's license number; or • Account number 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.
Individual notification requirements	An information holder must disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of Kentucky whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as required by law or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. Required notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. Required notification must be made promptly after the law enforcement agency determines that it will not compromise the investigation.
Regulator notification requirements	If a person discovers circumstances requiring notification of **more than 1,000 persons** at one time, the person must also notify, without unreasonable delay, all consumer reporting agencies and credit bureaus that compile and maintain files on consumers on a nationwide basis, as defined by 15 U.S.C. sec. 1681a, of the timing, distribution and content of the notices.

Enforcement	If a person discovers circumstances requiring notification of **more than 1,000 persons** at one time, the person must also notify, without unreasonable delay, all consumer reporting agencies and credit bureaus that compile and maintain files on consumers on a nationwide basis, as defined by 15 U.S.C. sec. 1681a, of the timing, distribution and content of the notices.

Louisiana

Statute (link)	La. Rev. Stat. § 51:3071 et seq.
What's a breach?	Breach of the security of the system means the compromise of the security, confidentiality or integrity of computerized data that results in or has a reasonable likelihood to result in the unauthorized acquisition of and access to personal information maintained by an agency or person. Good faith acquisition of personal information by an employee or agent of an agency or person for the purposes of the agency or person is not a breach of the security of the system, provided that the personal information is not used for or is subject to unauthorized disclosure.
What's considered personal information?	Personal information means the first name or first initial and last name of an individual resident of this state in combination with one or more of the following data elements when the name or the data element is not encrypted or redacted: • Social Security number; • Driver's license number or state identification card number; • 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; • Passport number; and • 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 characteristics, used by the owner or licensee to uniquely authenticate an individual's identity when the individual accesses a system or account. Personal information does not include publicly available information that is lawfully made available to the general public from federal, state or local government records.
Individual notification requirements	Any person or agency who owns or licenses computerized data that includes personal information must, following the discovery of a breach in the security of the system containing such data, notify any resident of the state whose personal information was or is reasonably believed to have been acquired by an unauthorized person. The notification required must be made in the most expedient time possible and without unreasonable delay but not later than **60 days** from discovery of the breach, consistent with any measures necessary to determine the scope of the breach, prevent further disclosures and restore the reasonable integrity of the data system. When notification is delayed by law enforcement request or due to a determination by the entity that measures are necessary to determine the scope of the breach, prevent further disclosures and restore the reasonable integrity of the data system, the entity must provide the attorney

	general the reasons for the delay in writing within the 60-day notification period. Upon receipt of the written reasons, the attorney general must allow a reasonable extension of time to provide the consumer notification. If a law enforcement agency determines that the notification required under this Section would impede a criminal investigation, such notification may be delayed until such law enforcement agency determines that the notification will no longer compromise such investigation.
Regulator notification requirements	The attorney general must be provided with the reasons for notification delay in writing within the 60-day notification period. However, if after reasonable investigation it is found that there is no reasonable likelihood of harm to the residents of the state, notification must not be required. The person or business must retain a copy of the written determination and supporting documentation for five years from the date of discovery of the breach of the security system. If requested in writing, the person or business must send a copy of the written determination and supporting documentation to the attorney general no later than 30 days from the date of receipt of the request.
Enforcement	Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful.

Maine

Statute (link)	10 Me. Rev. Stat. § 1346 et seq.
What's a breach?	Breach of the security of the system or "security breach" 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 of the individual maintained by a person. Good faith acquisition, release or use of personal information by an employee or agent of a person on behalf of the person is not a breach of the security of the system if the personal information is not used for or subject to further unauthorized disclosure to another person.
What's considered personal information?	Personal information means an individual's first name or first initial and last name in combination with one or more of the following data elements when either the name or the data elements are not encrypted or redacted: • Social Security number; • Driver's license number or state identification card number; • Account number, credit card number or debit card number, if circumstances exist wherein such a number could be used without additional identifying information, access codes or passwords; • Account passwords or personal identification numbers or other access codes; or • Any of the above data elements when not in connection with the individual's first name or first initial and last name, if the information is compromised would be sufficient to permit a person to fraudulently assume or attempt to assume the identity of the person whose information was compromised. Personal information does not include information from third-party claims databases maintained by property and casualty insurers or publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media.
Individual notification requirements	If an information broker that maintains computerized data that includes personal information becomes aware of a breach of the security of the system, they must conduct a good faith, reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused and must give notice of a breach of the security of the system following discovery or notification of the security breach to a resident of this state whose personal information has been or is reasonably believed to have been acquired by an unauthorized person. If any other person who maintains computerized data that includes personal information becomes aware of a breach of the security of the

	system, the person must conduct a good faith, reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused and must give notice of a breach of the security of the system following discovery or notification of the security breach to a resident of this state if misuse of the personal information has occurred or if it is reasonably possible that misuse will occur. The notices required must be made as expediently as possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or with measures necessary to determine the scope of the security breach and restore the reasonable integrity, security and confidentiality of the data in the system. If there is no delay of notification due to a law enforcement investigation, notice must be made no more than 30 days after the information broker or any other person maintaining computerized data becomes aware of a breach of security and identifies its scope.
Regulator notification requirements	If a person discovers a breach of the security of the system that requires notification to **more than 1,000 persons** at a single time, the person must also notify, without unreasonable delay, consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 United States Code, Section 1681a(p). Notification must include the date of the breach, an estimate of the number of persons affected by the breach, if known, and the actual or anticipated date that persons were or will be notified of the breach. When notice of a breach of the security of the system is required, the person must notify the appropriate state regulators within the Department of Professional and Financial Regulation, or if the person is not regulated by the department, the attorney general.
Enforcement	The appropriate state regulators within the Department of Professional and Financial Regulation will enforce this chapter for any person who is licensed or regulated by those regulators. The attorney general must enforce this chapter for all other persons.

Maryland

Statute (link)	Md. Code Com. Law § 14-3501 et seq.
What's a breach?	Breach of the security of a system means the unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of the personal information maintained by a business. A breach does not include the good faith acquisition of personal information by an employee or agent of a business for the purposes of the business, provided that the personal information is not used or subject to further unauthorized disclosure.
What's considered personal information?	Personal information means an individual's first name or first initial and last name in combination with one or more of the following data elements when the name or the data elements are not encrypted, redacted or otherwise protected by another method that renders the information unreadable or unusable: • A Social Security number, an Individual Taxpayer Identification Number, a passport number or other identification number issued by the federal government; • A driver's license number or state identification card number; • 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; • Health information, including information about an individual's mental health; • 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 • 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 characteristics, that can be used to uniquely authenticate the individual's identity when the individual accesses a system or account; or • A username or email address in combination with a password or security question and answer that permits access to an individual's email account. Personal information does not include: • Publicly available information that is lawfully made available to the general public from federal, state or local government records;

	• Information that an individual has consented to have publicly disseminated or listed; or • Information that is disseminated or listed in accordance with the federal Health Insurance Portability and Accountability Act.
Individual notification requirements	If a business discovers or is notified that it incurred a breach of the security system, it must conduct a good faith, reasonable and prompt investigation to determine the likelihood that personal information of the individual has been or will be misused as a result of the breach. Notification must be given as reasonably practicable but not later than **45 days** after the business concludes investigating. Notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation or jeopardize homeland or national security, or to determine the scope of the breach of the security of a system, identify the individuals affected or restore the integrity of the system. If there is a delay, notification must be given as soon as reasonably practicable but not later than 30 days after the law enforcement agency determines that it will not impede a criminal investigation and will not jeopardize homeland or national security.
Regulator notification requirements	Prior to giving the required notification to individuals, a business must provide notice of a breach of the security of a system to the Office of the Attorney General. If a business is required under § 14-3504 of Maryland Personal Information Protection Act to give notice of a breach of the security of a system to **1,000 or more individuals**, the business also must notify, without unreasonable delay, each consumer reporting agency that compiles and maintains files on consumers on a nationwide basis, as defined by 15 U.S.C. § 1681a(p), of the timing, distribution and content of the notices.
Enforcement	Violaters will be subject to the enforcement and penalty provisions contained under Title 13 Consumer Protection Act.

Massachusetts

Statute (link)	Mass. Gen. Laws 93H § 1 et seq.
What's a breach?	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 maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the commonwealth. A good faith but unauthorized acquisition of personal information by a person or agency or employee or agent thereof, for the lawful purposes of such person or agency, is not a breach of security unless the personal information is used in an unauthorized manner or subject to further unauthorized disclosure.
What's considered personal information?	Personal information means a resident's first name and last name or first initial and last name in combination with one or more of the following data elements that relate to such resident: • Social Security number; • Driver's license number or state-issued identification card number; or • 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. Personal information does not include information that is lawfully obtained from publicly available information or federal, state or local government records lawfully made available to the general public.
Individual notification requirements	A person or agency must provide notice, as soon as practicable and without unreasonable delay, when the person or agency knows or has reason to know of a breach of security or when the person or agency knows or has reason to know that the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose to the owner or licensor. Notice may be delayed if a law enforcement agency determines that notice may impede a criminal investigation and has notified the attorney general in writing and informs the person or agency of such determination. If notice is delayed due to such determination and as soon as the law enforcement agency determines and informs the person or agency that notification no longer poses a risk of impeding an investigation, notice must be provided as soon as practicable and without unreasonable delay.
Regulator notification requirements	Notice must be provided to the state attorney general and the director of consumer affairs and business regulation. The notice to be provided to the attorney general and the director of the office of consumer affairs and business regulation must consist of

	but not be limited to any steps the person or agency has taken or plans to take relating to the breach pursuant to the applicable federal law, rule, regulation, guidance or guidelines, provided further that if said person or agency does not comply with applicable federal laws, rules, regulations, guidance or guidelines, then it must be subject to the provisions of this chapter.
Enforcement	The attorney general may bring an action pursuant to section 4 of chapter 93A against a person or otherwise to remedy violations of this chapter and for other relief that may be appropriate.

Michigan

Statute (link)	**Mich. Comp. Laws § 445.63, 445.72 et seq.**
What's a breach?	Breach of the security of a database or "security breach" means the unauthorized access and acquisition of data that compromises the security or confidentiality of personal information maintained by a person or agency as part of a database of personal information regarding multiple individuals. Security breach does not include unauthorized access to data by an employee or other individual if the access meets all of the following: • The employee or other individual acted in good faith in accessing the data; • The access was related to the activities of the agency or person; and • The employee or other individual did not misuse any personal information or disclose any personal information to an unauthorized person.
What's considered personal information?	Personal identifying information means a name, number or other information that is used for the purpose of identifying a specific person or providing access to a person's financial accounts, including but not limited to a person's name, address, telephone number, driver's license or state personal identification card number, Social Security number, place of employment, employee identification number, employer or Taxpayer Identification Number, government passport number, health insurance identification number, mother's maiden name, demand deposit account number, savings account number, financial transaction device account number or the person's account password, any other account password in combination with sufficient information to identify and access the account, automated or electronic signature, biometrics, stock or other security certificate or account number, credit card number, vital record or medical records or information. Personal information means the first name or first initial and last name linked to one or more of the following data elements of a resident of this state: • Social Security number; • Driver's license number or state personal identification card number; or • Demand deposit or other financial account number or credit card or debit card number in combination with any required security code, access code or password that would permit access to any of the resident's financial accounts.
Individual notification requirements	Unless the person or agency determines that the security breach has not or is not likely to cause substantial loss or injury to or result in identity theft for one or more residents of this state, a person or

	agency that owns or licenses data included in a database that discovers a security breach or receives notice of a security breach must provide a notice of the security breach to each resident of this state who meets one or more of the following: • That resident's unencrypted and unredacted personal information was accessed and acquired by an unauthorized person; or • That resident's personal information was accessed and acquired in encrypted form by a person with unauthorized access to the encryption key. A person or agency must provide any notice required without unreasonable delay. A person or agency may delay providing notice without violating this requirement if either of the following is met: • A delay is necessary in order for the person or agency to take any measures necessary to determine the scope of the security breach and restore the reasonable integrity of the database. However, the agency or person must provide the required notice without unreasonable delay after the person or agency completes the measures necessary to determine the scope of the security breach and restore the reasonable integrity of the database; or • A law enforcement agency determines and advises the agency or person providing a notice that it will impede a criminal or civil investigation or jeopardize homeland or national security. However, the agency or person must provide the required notice without unreasonable delay after the law enforcement agency determines that providing the notice will no longer impede the investigation or jeopardize homeland or national security.
Regulator notification requirements	After a person or agency provides a notice, the person or agency must notify each consumer reporting agency that compiles and maintains files on consumers on a nationwide basis, as defined in 15 USC 1681a(p), of the security breach without unreasonable delay. A notification must include the number of notices the person or agency provided to residents of this state and the timing of those notices. This does not apply if the following is met: The person or agency is required to provide notice of a security breach to **1,000 or fewer** residents of this state.
Enforcement	Enforcement provides for criminal penalties for notice of a security breach that has not occurred, where such notice is given with the intent to defraud. The offense is a misdemeanor, punishable by imprisonment for not more than 30 days or a fine of not more than $250 per violation (or both). (The penalty is the same for second and third violations, except that the fine increases to $500 per violation and $750 per violation, respectively.) Similarly, entities who distribute

	an advertisement or make any other solicitation that misrepresents to the recipient that a security breach has occurred that may affect the recipient are punishable by imprisonment for not more than 93 days or a fine of not more than $1,000 per violation (or both). (The penalty is the same for second and third violations, except that the fine increases to $2,000 per violation and $3,000 per violation, respectively.)

Minnesota

Statute (link)	**Minn. Stat. § 325E.61 and 325E.64**
What's a breach?	Breach of the security system means unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security system, provided that the personal information is not used or subject to further unauthorized disclosure.
What's considered personal information?	Personal information means an individual's first name or first initial and last name in combination with one or more of the following data elements, when the data element is not secured by encryption or another method of technology that makes electronic data unreadable or unusable or was secured and the encryption key, password or other means necessary for reading or using the data was also acquired: • Social Security number; • Driver's license number or Minnesota identification card 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. Personal information does not include publicly available information that is lawfully made available to the general public from federal, state or local government records.
Individual notification requirements	Any person or business that conducts business in this state and owns or licenses data that includes personal information must disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. The disclosure 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, identify the individuals affected and restore the reasonable integrity of the data system.
Regulator notification requirements	If a person discovers circumstances requiring notification of **more than 500 persons** at one time, the person must also notify, **within 48 hours**, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by United States Code, title 15, section 1681a, of the timing, distribution and content of the notices.
Enforcement	The attorney general must enforce this section under section 8.31.

Mississippi

Statute (link)	**Miss. Code § 75-24-29**
What's a breach?	Breach of security means unauthorized acquisition of electronic files, media, databases or computerized data containing personal information of any resident of this state 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.
What's considered personal information?	Personal information means an individual's first name or first initial and last name in combination with one or more of the following data elements: • Social Security number; • Driver's license number, state identification card number or tribal identification card number; or • 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. Personal information does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media. Affected individual means any individual who is a resident of this state whose personal information was or is reasonably believed to have been intentionally acquired by an unauthorized person through a breach of security.
Individual notification requirements	A person who conducts business in this state must disclose any breach of security to all affected individuals. The disclosure must be made without unreasonable delay, subject to all legal requirements and to the completion of an investigation by the person to determine the nature and scope of the incident, identify the affected individuals or restore the reasonable integrity of the data system. After an appropriate investigation, notification is not required if the person reasonably determines that the breach will not likely result in harm to the affected individuals. Any required notification must be delayed for a reasonable period of time if a law enforcement agency determines that the notification will impede a criminal investigation or national security and the law enforcement agency has made a request for the notification to be delayed.
Regulator notification requirements	*No information about these requirements is available at this time.*
Enforcement	Failure to comply with data breach notification requirements constitutes an unfair trade practice and will be enforced by the

	attorney general. However, nothing in this section may be construed to create a private right of action.

Missouri

Statute (link)	Mo. Rev. Stat. § 407.1500
What's a breach?	A breach is an unauthorized access to and unauthorized acquisition of personal information maintained in computerized form by a person who compromises the security, confidentiality or integrity of the personal information. Good faith acquisition of personal information by a person or that person's employee or agent for a legitimate purpose of that person is not a breach of security, provided that the personal information is not used in violation of applicable law or in a manner that harms or poses an actual threat to the security, confidentiality or integrity of the personal information.
What's considered personal information?	Personal information means 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 if any of the data elements are not encrypted, redacted or otherwise altered by any method or technology in a manner that makes the name or data elements are unreadable or unusable: • Social Security number; • Driver's license number or other unique identification number created or collected by a government body; • 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; • Unique electronic identifier or routing code, in combination with any required security code, access code or password that would permit access to an individual's financial account; • Medical information; or • Health insurance information. Personal information does not include information that is lawfully obtained from publicly available sources or from federal, state or local government records lawfully made available to the general public.
Individual notification requirements	Any person who owns or licenses personal information of the residents of Missouri or any person who conducts business in Missouri that owns or licenses personal information in any form of a resident of Missouri must provide notice to the affected consumer that there has been a breach of security following discovery or notification of the breach. The disclosure notification must be made without unreasonable delay and: • Consistent with the legitimate 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. After an appropriate investigation by the person or after consultation with the relevant federal, state or local agencies responsible for law enforcement, notification is not required if the person determines that a risk of identity theft or other fraud to any consumer is not reasonably likely to occur as a result of the breach. Such a determination must be documented in writing, and the documentation must be maintained for five years.
Regulator notification requirements	In the event a person provides notice to **more than 1,000 consumers** at one time, the person must notify, without unreasonable delay, the attorney general's office and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. Section 1681a(p), of the timing, distribution and content of the notice.
Enforcement	The attorney general has exclusive authority to bring an action to obtain actual damages for a willful and knowing violation and may seek a civil penalty not to exceed $150,000 per breach of the security of the system or a series of breaches of a similar nature that are discovered in a single investigation.

Montana

Statute (link)	**Mont. Code § 30-14-1704 et seq., 33-19-321**
What's a breach?	Breach of the security of a data system or "breach" means the unauthorized acquisition of computerized data that: • Materially compromises the security, confidentiality or integrity of the personal information maintained by a state agency or by a third party on behalf of a state agency; and • Causes or is reasonably believed to cause loss or injury to a person.
What's considered personal information?	Personal information means a first name or first initial and last name in combination with one or more of the following data elements when the name and data elements are not encrypted: • A Social Security number; • A driver's license number, an identification card number issued pursuant to 61-12-501, a tribal identification number or enrollment number or a similar identification number issued by any state, the District of Columbia, the Commonwealth of Puerto Rico, Guam, the Virgin Islands or American Samoa; • 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 a person's financial account; • Medical record information as defined in 33-19-104; • A taxpayer identification number; or • An identity protection personal identification number issued by the United States Internal Revenue Service. Personal information does not include publicly available information from federal, state, local or tribal government records.
Individual notification requirements	Any person or business that conducts business in Montana and owns or licenses computerized data that includes personal information must disclose any breach of the security of the data system following discovery or notification of the breach to any resident of Montana whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. The disclosure must be made 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. Required notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation and requests a delay in notification. Required notification must be made after the law enforcement agency determines that it will not compromise the investigation.

Regulator notification requirements	If a business discloses a security breach to any individual and gives notice to the individual that suggests, indicates or implies to the individual that the individual may obtain a copy of the file on the individual from a consumer credit reporting agency, the business must coordinate with the consumer reporting agency as to the timing, content and distribution of the notice to the individual. The coordination may not unreasonably delay the notice to the affected individuals. Any person or business that is required to issue a notification must simultaneously submit an electronic copy of the notification and a statement providing the date and method of distribution of the notification to the attorney general's consumer protection office, excluding any information that personally identifies any individual who is entitled to receive a notification. If a notification is made to more than one individual, a single copy of the notification must be submitted that indicates the number of individuals in the state who received notification.
Enforcement	An individual who is adversely affected by a violation of 30-14-1712(1) may bring an action against an individual or a business that has directly violated 30-14-1712(1) for the greater of three times actual damages or $5,000 for each violation.

Nebraska

Statute (link)	Neb. Rev. Stat. § 87-801 et seq.
What's a breach?	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 an individual or a commercial entity. Good faith acquisition of personal information by an employee or agent of an individual or a commercial entity for the purposes of the individual or the commercial entity is not a breach of the security of the system if the personal information is not used or subject to further unauthorized disclosure. In addition, the acquisition of personal information pursuant to a search warrant, subpoena or other court order or pursuant to a subpoena or order of a state agency is not a breach of the security of the system.
What's considered personal information?	A Nebraska resident's first name or first initial and last name in combination with one or more of the following data elements that relate to the resident if either the name or the data elements are not encrypted, redacted or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable: • Social Security number; • Motor vehicle operator's license number or state identification card number; • Account number or credit or debit card number in combination with any required security code, access code or password that would permit access to a resident's financial account; • Unique electronic identification number or routing code, in combination with any required security code, access code or password; or • Unique biometric data, such as a fingerprint, voiceprint or retina or iris image or other unique physical representation; or • A username or email address, in combination with a password or security question and answer, that would permit access to an online account. Personal information does not include publicly available information that is lawfully made available to the general public from federal, state or local government records.
Individual notification requirements	An individual or a commercial entity that conducts business in Nebraska and owns or licenses computerized data that includes personal information about a resident of Nebraska must, when it becomes aware of a breach of the security of the system, conduct in good faith a reasonable and prompt investigation to determine the likelihood that 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 individual or commercial entity must give notice to the affected Nebraska resident. Notice must be made as soon as 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. Notice may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation. Notice must be made in good faith, without unreasonable delay and as soon as possible after the law enforcement agency determines that notification will no longer impede the investigation.
Regulator notification requirements	If notice of a breach of security of the system is required, the individual or commercial entity must also provide notice of the breach of security of the system to the attorney general not later than the time when notice is provided to the Nebraska resident.
Enforcement	For purposes of the Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006, the attorney general may issue subpoenas and seek and recover direct economic damages for each affected Nebraska resident injured by a violation of section 87-803. A violation of section 87-808 must be considered a violation of section 59-1602 and be subject to the Consumer Protection Act and any other law which provides for the implementation and enforcement of section 59-1602. A violation of section 87-808 does not give rise to a private cause of action.

Nevada

Statute (link)	Nev. Rev. Stat. § 603A.010 et seq., 242.183
What's a breach?	Breach of the security of the system data means unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information maintained by the data collector. A breach does not include the good faith acquisition of personal information by an employee or agent of the data collector for a legitimate purpose of the data collector so long as the personal information is not used for a purpose unrelated to the data collector or subject to further unauthorized disclosure.
What's considered personal information?	Personal information means a natural person's first name or first initial and last name in combination with one or more of the following data elements when the name and data elements are not encrypted: • Social Security number; • Driver's license number, driver authorization card number or identification card number; • Account number, credit card number or debit card number in combination with any required security code, access code or password that would permit access to the person's financial account; • A medical identification number or a health insurance identification number; or • A username, 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. The term does not include the last four digits of a Social Security number, driver's license number, driver authorization card number or identification card number, nor publicly available information that is lawfully made available to the general public from federal, state or local governmental records.
Individual notification requirements	Any data collector that owns or licenses computerized data that includes personal information must disclose any breach of the security of the system data following discovery or notification to any resident of Nevada whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as required by law or by any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system data. Required notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation.

	However, notification must be made after the law enforcement agency determines that the notification will not compromise the investigation.
Regulator notification requirements	If a data collector determines that notification is required to be given to **more than 1,000 persons** at any one time, the data collector must also notify, without unreasonable delay, any consumer reporting agency, as that term is defined in 15 U.S.C. § 1681a(p), that compiles and maintains files on consumers on a nationwide basis, of the time the notification is distributed and the content of the notification.
Enforcement	A data collector that provides the notification required pursuant to NRS 603A.220 may commence an action for damages against a person who unlawfully obtained or benefited from personal information obtained from records maintained by the data collector. A data collector that prevails in such an action may be awarded damages, which may include, without limitation, the reasonable costs of notification, reasonable attorney's fees and costs and punitive damages when appropriate. The costs of notification include, without limitation, labor, materials, postage and any other costs reasonably related to providing the notification. If the attorney general or a district attorney of any county has reason to believe that any person is violating, proposes to violate or has violated the provisions of NRS 603A.010 to 603A.290, inclusive, the attorney general or district attorney may bring an action against that person to obtain a temporary or permanent injunction against the violation.

New Hampshire

Statute (link)	**N.H. Rev. Stat. § 359-C:19 et seq.**
What's a breach?	Security breach means unauthorized acquisition of computerized data that compromises the security or confidentiality of personal information maintained by a person doing business in this state. Good faith acquisition of personal information by an employee or agent of a person for the purposes of the person's business must not be considered a security breach, provided that the personal information is not used or subject to further unauthorized disclosure.
What's considered personal information?	Personal information means an individual's first name or initial and last name in combination with one or more of the following data elements when either the name or the data elements are not encrypted: • Social Security number; • Driver's license number or other government identification number; • Account number, credit card number or debit card number in combination with any required security code, access code or password that would permit access to an individual's financial account. Personal information does not include information that is lawfully made available to the general public from federal, state or local government records.
Individual notification requirements	Any person doing business in New Hampshire who owns or licenses computerized data that includes personal information must, when it becomes aware of a security breach, 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 person must notify the affected individuals as soon as possible as required under this subdivision.
Regulator notification requirements	If a person is required to notify **more than 1,000 consumers** of a breach of security, the person must also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by 15 U.S.C. section 1681a(p), of the anticipated date of the notification to the consumers, the approximate number of consumers who will be notified and the content of the notice. Nothing in this paragraph must be construed to require the person to provide to any consumer reporting agency the names of the consumers entitled to receive the notice or any personal information relating to them.
Enforcement	Any person injured by any violation under this subdivision may bring an action for damages and such equitable relief, including an injunction, as the court deems necessary and proper.

	If the court finds in favor of the plaintiff, recovery will be in the amount of actual damages. If the court finds that the act or practice was a willful or knowing violation of this chapter, it will award as much as three times but not less than two times such amount. In addition, a prevailing plaintiff will be awarded the costs of the suit and reasonable attorney's fees, as determined by the court. Any attempted waiver of the right to the damages set forth in this paragraph will be void and unenforceable. Injunctive relief will be available to private individuals under this chapter without bond, subject to the discretion of the court. The New Hampshire attorney general's office will enforce the provisions of this subdivision pursuant to RSA 358-A:4.

New Jersey

Statute (link)	N.J. Stat. § 56:8-163
What's a breach?	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. Good faith acquisition of personal information by an employee or agent of the business for a legitimate business purpose is not a breach of security, provided that the personal information is not used for a purpose unrelated to the business or subject to further unauthorized disclosure.
What's considered personal information?	Personal information means an individual's first name or first initial and last name linked with one or more of the following data elements: • Social Security number; • Driver's license number or state identification card 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. 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. Personal information does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media.
Individual notification requirements	Any business that conducts business in New Jersey or any public entity that compiles or maintains computerized records that include personal information must disclose any breach of security of those computerized records following discovery or notification of the breach to any customer who is a resident of New Jersey whose personal information was or is reasonably believed to have been accessed by an unauthorized person. The disclosure to a customer 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. Disclosure of a breach of security to a customer is not be required if the business or public entity establishes that misuse of the information is not reasonably possible. Any determination must be documented in writing and retained for five years. Required notification must be delayed if a law enforcement agency determines that the notification will impede a criminal or civil

	investigation and that agency has made a request for the notification to be delayed. The required notification must be made after the law enforcement agency determines that its disclosure will not compromise the investigation and notifies that business or public entity.
Regulator notification requirements	Any business or public entity required to disclose a breach of security of a customer's personal information must, in advance of the disclosure to the customer, report the breach of security and any information pertaining to the breach to the Division of State Police in the Department of Law and Public Safety for investigation or handling, which may include dissemination or referral to other appropriate law enforcement entities. In addition to any other disclosure or required notification, in the event that a business or public entity discovers circumstances requiring notification **of more than 1,000 persons** at one time, the business or public entity must also notify, without unreasonable delay, all consumer reporting agencies that compile or maintain files on consumers on a nationwide basis, as defined by subsection (p) of section 603 of the federal "Fair Credit Reporting Act" (15 U.S.C. s.1681a), of the timing, distribution and content of the notices.
Enforcement	It is an unlawful practice and a violation of P.L.1960, c.39 (C.56:8-1 et seq.) to willfully, knowingly or recklessly violate sections 10 through 13 of this amendatory and supplementary act.

New Mexico

Statute (link)	N.M. Stat. 57-12C-1
What's a breach?	Security breach means the unauthorized acquisition of unencrypted computerized data or 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. Security breach does not include the good faith acquisition of personal identifying information by an employee or agent of a person for a legitimate business purpose of the person, provided that the personal identifying information is not subject to further unauthorized disclosure.
What's considered personal information?	Personal identifying information means an individual's first name or first initial and last name in combination with one or more of the following data elements that relate to the individual when the data elements are not protected through encryption or redaction or otherwise rendered unreadable or unusable: • Social Security number; • Driver's license number or government-issued identification number; • Account number, credit card number or debit card number in combination with any required security code, access code or password that would permit access to a person's financial account; or • Biometric data. Personal identifying information does not mean information that is lawfully obtained from publicly available sources or from federal, state or local government records lawfully made available to the general public.
Individual notification requirements	A person who owns or licenses elements that include personal identifying information of a New Mexico resident must provide notification to each New Mexico resident whose personal identifying information is reasonably believed to have been subject to a security breach. Notification must be made in the most expedient time possible but not later than **45 calendar days** following the discovery of the security breach, except as provided in Section 9 [57-12C-9 NMSA 1978] of the Data Breach Notification Act.
Regulator notification requirements	A person who is required to issue notification of a security breach pursuant to the Data Breach Notification Act to **more than 1,000 New Mexico residents** as a result of a single security breach must notify the office of the attorney general and major consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. Section 1681a(p), of the security breach in the most expedient time possible and no later than

	45 calendar days, except as provided in Section 9 [57-12C-9 NMSA 1978] of the Data Breach Notification Act. A person required to notify the attorney general and consumer reporting agencies must notify the attorney general of the number of New Mexico residents that received notification pursuant to Section 6 of that act [57-12C-6 NMSA 1978] and must provide a copy of the notification that was sent to affected residents within 45 calendar days following the discovery of the security breach, except as provided in Section 9 of the Data Breach Notification Act.
Enforcement	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 behalf of individuals and in the name of the state alleging a violation of that act. In any action filed by the attorney general pursuant to the Data Breach Notification 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 Data Breach Notification Act 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 (link)	N.Y. Gen. Bus. Law § 899-aa
What's a breach?	Breach of the security of the system means unauthorized access to or acquisition of computerized data that compromises the security, confidentiality or integrity of private information maintained by a business. Good faith access to or acquisition of private information by an employee or agent of the business for the purposes of the business is not a breach of the security of the system, provided that the private information is not used or subject to unauthorized disclosure.
What's considered personal information?	Personal information means any information concerning a natural person which, because of name, number, personal mark or another identifier, can be used to identify that natural person. Private information means either personal information consisting of any information in combination with one or more of the following data elements when either the data element or the combination of personal information plus the data element is not encrypted or is encrypted with an encryption key that has also been accessed or acquired: • Social Security number; • Driver's license number or nondriver identification card number; • 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; • Account number, credit or debit card number, if circumstances exist wherein such a number could be used to access an individual's financial account without additional identifying information, security code, access code or password; • Biometric information, meaning data generated by electronic measurements of an individual's unique physical characteristics, such as a fingerprint, voiceprint, retina or iris image or other unique physical representation or digital representation of biometric data, which are used to authenticate or ascertain the individual's identity; or • A username or email address in combination with a password or security question and answer that would permit access to an online account.
Individual notification requirements	Any person or business which owns or licenses computerized data that includes private information must 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. The disclosure 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 integrity of the system.
Regulator notification requirements	If the incident affects **over 500 residents of New York**, the person or business must provide the written determination to the state attorney general within 10 days after the determination. If notice of the breach of the security of the system is made to affected persons pursuant to the breach notification as required by law, no additional notice to those affected persons is required. However, notice still must be provided to the state attorney general, the department of state and the division of state police and to consumer reporting agencies. In the event that **more than 5,000 New York residents** are to be notified at one time, the person or business must also notify consumer reporting agencies as to the timing, content and distribution of the notices and the approximate number of affected persons. This notice must be made without delaying notice to affected New York residents.
Enforcement	Whenever the attorney general believes from evidence that there is a violation of data breach notification requirements, he or she may bring an action in the name and on behalf of the people of the state of New York, in a court of justice having jurisdiction to issue an injunction, to enjoin and restrain the continuation of such violation.

North Carolina

Statute (link)	N.C. Gen. Stat. §§ 75-61, 75-65
What's a breach?	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, is reasonably likely to occur or creates a material risk of harm to a consumer. Any incident of unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential process or key constitutes a security breach. Good faith acquisition of personal information by an employee or agent of the business for a legitimate purpose is not a security breach, provided that the personal information is not used for a purpose other than a lawful purpose of the business and is not subject to further unauthorized disclosure.
What's considered personal information?	Personal information means a person's first name or first initial and last name in combination with identifying information as defined in G.S. 14-113.20(b). Personal information does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, including name, address and telephone number, and does not include information made lawfully available to the general public from federal, state or local government records.
Individual notification requirements	Any business that owns or licenses personal information of residents of North Carolina or any business that conducts business in North Carolina that owns or licenses personal information in any form (whether computerized, paper or otherwise) must provide notice to the affected person that there has been a security breach following discovery or notification of the breach. The disclosure notification must be made without unreasonable delay, consistent with the legitimate needs of law enforcement, as required by law and consistent with any measures necessary to: • Determine sufficient contact information; • Determine the scope of the breach; and • Restore the reasonable integrity, security and confidentiality of the data system. Personal information does not include electronic identification numbers, electronic mail names or addresses, internet account numbers, internet identification names, parent's legal surname prior to marriage or a password unless this information would permit access to a person's financial account or resources. The required notice must 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 a request is made in writing or the business documents such

	request contemporaneously in writing, including the name of the law enforcement officer making the request and the officer's law enforcement agency engaged in the investigation. The required notice must be provided without unreasonable delay after the law enforcement agency communicates to the business its determination that notice will no longer impede the investigation or jeopardize national or homeland security.
Regulator notification requirements	In the event a business provides notice to an affected person, the business must notify without unreasonable delay the Consumer Protection Division of the attorney general's office of the nature of the breach, the number of consumers affected by the breach, steps taken to investigate the breach, steps taken to prevent a similar breach in the future and information regarding the timing, distribution and content of the notice. In the event a business provides notice to **more than 1,000 persons** at one time, the business must 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, as defined in 15 U.S.C. § 1681a(p), of the timing, distribution and content of the notice.
Enforcement	A violation of data breach notification requirements is a violation of G.S. 75-1.1. No private right of action may be brought by an individual unless such individual is injured as a result of the violation.

North Dakota

Statute (link)	N.D. Cent. Code § 51-30-01 et seq.
What's a breach?	Breach of the security system means unauthorized acquisition of computerized data when access to personal information has not been secured by encryption or by any other method or technology that renders the electronic files, media or databases unreadable or unusable. Good faith acquisition of personal information by an employee or agent of the person is not a breach of the security of the system if the personal information is not used or subject to further unauthorized disclosure.
What's considered personal information?	Personal information means an individual's first name or first initial and last name in combination with any of the following data elements when the name and the data elements are not encrypted: • The individual's Social Security number; • The operator's license number assigned to an individual by the department of transportation under section 39-06-14; • A nondriver color photo identification card number assigned to the individual by the department of transportation under section 39-06-03.1; • The individual's financial institution account number, credit card number or debit card number in combination with any required security code, access code or password that would permit access to an individual's financial accounts; • The individual's date of birth; • The maiden name of the individual's mother; • Medical information; • Health insurance information; • An identification number assigned to the individual by the individual's employer in combination with any required security code, access code or password; or • The individual's digitized or other electronic signature. Personal information does not include publicly available information that is lawfully made available to the general public from federal, state or local government records.
Individual notification requirements	Any person who owns or licenses computerized data that includes personal information must disclose any breach of the security system following discovery or notification of the breach in the security of the data to any resident of the state whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. The notification required by this chapter may be delayed if a law enforcement agency determines that the notification will impede a

	criminal investigation. The notification required by this chapter must be made after the law enforcement agency determines that the notification will not compromise the investigation.
Regulator notification requirements	Any person who experiences a breach of the security system must disclose to the attorney general by mail or electronic mail any breach of the security system that **exceeds 250 individuals**. The disclosure 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 to restore the integrity of the data system.
Enforcement	The attorney general may enforce this chapter. The attorney general has all the powers and may seek all the remedies provided by law.

Ohio

Statute (link)	**Ohio Rev. Code § 1347.12, 1349.19, 1349.191, 1349.192**
What's a breach?	Breach of the security of the system means 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, is reasonably believed to have caused, or is reasonably believed will cause a material risk of identity theft or other fraud to the person or property of a resident of this state.
What's considered personal information?	Personal information means an individual's name, consisting of the individual's first name or first initial and last name, in combination with and linked to one or more of the following data elements when the data elements are not encrypted, redacted or altered by any method or technology in such a manner that the data elements are unreadable: • Social Security number; • Driver's license number or state identification card number; • 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. Personal information does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or any of the following media that are widely distributed, including any: • News, editorial or advertising statement published in any bona fide newspaper, journal or magazine or broadcast over radio or television; • Information or news gathered or furnished by any bona fide reporter, correspondent or news bureau to news media; • Publication designed for and distributed to members of any bona fide association or charitable or fraternal nonprofit corporation; or • Type of media similar in nature to any item, entity or activity identified above.
Individual notification requirements	Any person who owns or licenses computerized data that includes personal information must disclose any breach of the security of the system, following its discovery or notification of the breach of the security of the system, to any resident of this state whose personal information was or reasonably is believed to have been, accessed and acquired by an unauthorized person if the access and acquisition by the unauthorized person causes or reasonably is believed will cause a material risk of identity theft or other fraud to the resident.

	The disclosure described above may be made pursuant to any provision of a contract entered into by the person with another person prior to the date the breach of the security of the system occurred if that contract does not conflict with nor waives any provision of data breach notification requirements. A resident of this state is an individual whose principal mailing address is reflected in the records of the person is in this state. The person must make the disclosure in the most expedient time possible but not later than **45 days** following its discovery or notification of the breach in the security of the system, subject to the legitimate needs of law enforcement activities 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. The person may delay the disclosure or notification required if a law enforcement agency determines that the disclosure or notification will impede a criminal investigation or jeopardize homeland or national security. In this case, the person must make the disclosure or notification after the law enforcement agency determines that disclosure or notification will not compromise the investigation or jeopardize homeland or national security.
Regulator notification requirements	If a person discovers circumstances that require disclosure to **more than 1,000 residents** of this state involved in a single occurrence of a breach of the security of the system, the person must notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution and content of the disclosure given by the person to the residents of this state. In no case must a person who is required to make a notification to the consumer reporting agencies mentioned above delay any required disclosure or notification to affected individuals in order to make the notification to the consumer reporting agencies.
Enforcement	The attorney general may conduct an investigation and bring a civil action upon an alleged failure by a person to comply with the requirements of this data breach notification laws.

Oklahoma

Statute (link)	24 Okla. Stat. § 161 et seq.
What's a breach?	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 or the individual or entity reasonably believes has caused or will cause identity theft or other fraud to any resident of this state. Good faith acquisition of personal information by an employee or agent of an individual or entity for the purposes of the individual or the entity is not a breach of the security of the system, provided that the personal information is not used for a purpose other than a lawful purpose of the individual or entity or subject to further unauthorized disclosure.
What's considered personal information?	Personal information means the first name or first initial and last name in combination with and linked to 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: • Social Security number, • Driver's license number or state identification card number issued in lieu of a driver's license; or • 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 the financial accounts of a resident. Personal information does not include information that is lawfully obtained from publicly available information or from federal, state or local government records lawfully made available to the general public.
Individual notification requirements	An individual or entity that owns or licenses computerized data that includes personal information must disclose any breach of the security of the system following discovery or notification of the breach of the security of the system to any resident of this state 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 the individual or entity reasonably believes has caused or will cause identity theft or other fraud to any resident of this state. The disclosure must be made without unreasonable delay unless an exemption applies or in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the system. Notice required may be delayed if a 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. Required notice must be made without unreasonable delay

	after the law enforcement agency determines that notification will no longer impede the investigation or jeopardize national or homeland security.
Regulator notification requirements	*No information about regulator notification requirements is available at this time.*
Enforcement	A violation of data breach notification requirements 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 if they result in injury or loss to residents of this state. The attorney general or a district attorney has exclusive authority to bring action and may obtain either actual damages for a violation of this act 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 (link)	**Or. Rev. Stat. §§ 646A.600, 646A.602, 646A.604, 646A.624, 646A.626**
What's a breach?	Breach of security means unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information that a person maintains or possesses. Breach of security does not include an inadvertent acquisition of personal information by a person or the person's employee or agent if the personal information is not used in violation of applicable law or in a manner that harms or poses an actual threat to the security, confidentiality or integrity of the personal information.
What's considered personal information?	Personal information means a consumer's first name or first initial and last name in combination with one or more of the following data elements if encryption, redaction or other methods have not rendered the data elements unusable or if the data elements are encrypted and the encryption key has been acquired: • A consumer's Social Security number; • A consumer's driver's license number or state identification card number issued by the Department of Transportation; • A consumer's passport number or other identification number issued by the United States; • A consumer's 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; • Data from automatic measurements of a consumer's physical characteristics, such as an image of a fingerprint, retina or iris, that are used to authenticate the consumer's identity in the course of a financial transaction or other transaction; • A consumer's health insurance policy number or health insurance subscriber identification number in combination with any other unique identifier that a health insurer uses to identify the consumer; • Any information about a consumer's medical history or mental or physical condition or about a health care professional's medical diagnosis or treatment of the consumer; • A username or other means of identifying a consumer for the purpose of permitting access to the consumer's account, together with any other method necessary to authenticate the username or means of identification; or

	• Any of the data elements or any combination of the data elements described above without the consumer's username or the consumer's first name or first initial and last name, if:
	  ○ Encryption, redaction or other methods have not rendered the data element or combination of data elements unusable; and
	  ○ The data element or combination of data elements would enable a person to commit identity theft against a consumer.
	
	Personal information does not include information in a federal, state or local government record, other than a Social Security number, that is lawfully made available to the public.

Individual notification requirements	A vendor that discovers a breach of security or has reason to believe that a breach of security has occurred must notify a covered entity with which the vendor has a contract as soon as is practicable but not later than **10 days** after discovering the breach of security or having a reason to believe that the breach of security occurred. A covered entity must give notice of a breach of security in the most expeditious manner possible, without unreasonable delay but not later than **45 days** after discovering or receiving notification of the breach of security. A covered entity may delay giving the notice only if a law enforcement agency determines that notification will impede a criminal investigation and if the law enforcement agency requests in writing that the covered entity delay the notification.
Regulator notification requirements	If a covered entity discovers or receives notice of a breach of security that affects **more than 1,000 consumers**, the covered entity must notify, without unreasonable delay, all consumer reporting agencies that compile and maintain reports on consumers on a nationwide basis of the timing, distribution and content of the notice the covered entity gave to affected consumers and must include in the notice any police report number assigned to the breach of security. A covered entity may not delay notifying affected consumers of a breach of security in order to notify consumer reporting agencies.
Enforcement	A person's violation of data breach notification requirements is an unlawful practice under ORS 646.607.

Pennsylvania

Statute (link)	**73 Pa. Stat. § 2301 et seq.**
What's a breach?	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.

	Good faith acquisition of personal information by an employee or agent of the entity for the purposes of the entity is not a breach of the security of the system if the personal information is not used for a purpose other than the lawful purpose of the entity and is not subject to further unauthorized disclosure.
What's considered personal information?	Personal information means an individual's first name or first initial and last name in combination with and linked to one or more of the following data elements when the data elements are not encrypted or redacted: • Social Security number; • Driver's license number or a state identification card number issued in lieu of a driver's license; or • 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. Personal information does not include publicly available information that is lawfully made available to the general public from federal, state or local government records.
Individual notification requirements	An entity that maintains, stores or manages computerized data that includes personal information must provide notice of any breach of the security of the system following discovery of the breach of the security of the system to any Pennsylvania resident whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person. In order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system, the notice must be made without unreasonable delay. A Pennsylvania resident may be determined to be an individual whose principal mailing address, as reflected in the computerized data maintained, stored or managed by the entity, is within the state. The required notification may be delayed if a law enforcement agency determines and advises the entity in writing (specifically referencing the pertinent data breach notification section) that the notification will impede a criminal or civil investigation. The required notification must be made after the law enforcement agency determines that it will not compromise the investigation or national or homeland security.
Regulator notification requirements	When an entity provides notification under this act to **more than 1,000 persons** 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, as defined in section 603 of the Fair Credit Reporting Act (Public Law 91-508, 15 U.S.C. § 1681a), of the timing, distribution and number of notices.
Enforcement	The attorney general has exclusive authority to bring an action under the Unfair Trade Practices and Consumer Protection Law for a violation of data breach notification laws.

Rhode Island

Statute (link)	R.I. Gen. Laws § 11-49.2-1 et seq.
What's a breach?	Breach of the security of the system means unauthorized access or acquisition of unencrypted, computerized data information that compromises the security, confidentiality or integrity of personal information maintained by the municipal agency, state agency or person. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.
What's considered personal information?	Personal information means an individual's first name or first initial and last name in combination with one or more of the following data elements, when the name and the data elements are not encrypted or are in hard copy, paper format: • Social Security number; • Driver's license number, Rhode Island identification card number or tribal identification number; • Account number, credit or debit card number, in combination with any required security code, access code, password or personal identification number, that would permit access to an individual's financial account; • Medical or health insurance information; or • Email address with any required security code, access code or password that would permit access to an individual's personal, medical, insurance or financial account. Personal information does not include publicly available information that is lawfully made available to the general public from federal, state or local government records.
Individual notification requirements	The notification must be made in the most expedient time possible, but no later than **45 calendar days** after confirmation of the breach and the ability to ascertain the information required to fulfill notice requirements and must be consistent with the legitimate needs of law enforcement. Required notification may be delayed if a federal, state or local law enforcement agency determines that the notification will impede a criminal investigation. The federal, state or local law enforcement agency must notify the municipal agency, state agency or the person of the request to delay notification without unreasonable delay. If notice is delayed due to such determination, then as soon as the federal, state or municipal law enforcement agency determines and informs the municipal agency, state agency or person who notification no longer poses a risk of impeding an investigation, notice must be provided as soon as practicable. The municipal agency, state agency

	or person must cooperate with federal, state or municipal law enforcement in its investigation of any breach of security or unauthorized acquisition or use, which must include the sharing of information relevant to the incident. This is provided, however, that such disclosure must not require the disclosure of confidential business information or trade secrets.
Regulator notification requirements	In the event that **more than 500 Rhode Island residents** are to be notified, the municipal agency, state agency or person must notify the attorney general and the major credit reporting agencies as to the timing, content and distribution of the notices and the approximate number of affected individuals. Notification to the attorney general and the major credit reporting agencies must be made without delaying notice to affected Rhode Island residents.
Enforcement	Each reckless violation of this chapter is a civil violation for which a penalty of not more than $100 per record may be adjudged against a defendant. Each knowing and willful violation of this chapter is a civil violation for which a penalty of not more than $200 per record may be adjudged against a defendant. Whenever the attorney general has reason to believe that a violation of these requirements has occurred and that proceedings would be in the public interest, the attorney general may bring an action in the name of the state against the business or person in violation.

South Carolina

Statute (link)	S.C. Code § 39-1-90
What's a breach?	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. Good faith acquisition of personal identifying information by an employee or agent of the person for the purposes of its business is not a breach of the security of the system if the personal identifying information is not used or subject to further unauthorized disclosure.
What's considered personal information?	Personal identifying information means the first name or first initial and last name in combination with and linked to 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: • Social Security number; • Driver's license number or state identification card number issued instead of a driver's license; • 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 account; or • 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 will uniquely identify an individual.
Individual notification requirements	A person conducting business in South Carolina and owning or licensing computerized data or other data that includes personal identifying information must disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of 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. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as required by law or with measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

Regulator notification requirements	If a business provides notice to **more than 1,000 persons** at one time, the business must 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, as defined in 15 USC Section 1681a(p), of the timing, distribution and content of the notice.
Enforcement	A person who knowingly and willfully violates data breach notification requirements is subject to an administrative fine in the amount of $1,000 for each resident whose information was accessible due to the breach, the amount to be decided by the Department of Consumer Affairs.

South Dakota

Statute (link)	SDCL §§ 22-40-19 to 22-40-26
What's a breach?	Breach of system security means the unauthorized acquisition of unencrypted computerized data or encrypted computerized data and the encryption key by any person who materially compromises the security, confidentiality or integrity of personal or protected information maintained by the information holder. A breach does not include the good faith acquisition of personal or protected information by an employee or agent of the information holder for the purposes of the information holder if the personal or protected information is not used or subject to further unauthorized disclosure.
What's considered personal information?	Personal information means a person's first name or first initial and last name, in combination with one or more of the following data elements: • Social Security number; • Driver's license number or other unique identification number created or collected by a government body; • 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; • Health information as defined in 45 CFR 160.103; or • An identification number assigned to a person by the person's employer in combination with any required security code, access code, password or biometric data generated from measurements or analysis of human body characteristics for authentication purposes. Personal information does not include information that is lawfully made available to the general public from federal, state or local government records or information that has been redacted or otherwise made unusable.
Individual notification requirements	Following the discovery by or notification to an information holder of a breach of system security, an information holder must 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. A disclosure must be made no later than **60 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 as provided under § 22-40-21. An information holder is not required to make a disclosure 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 must document the determination in writing and maintain the documentation for not less than three years. A notification required under § 22-40-20 may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. If the notification is delayed, the notification must be made no later than 30 days after the law enforcement agency determines that notification will not compromise the criminal investigation.
Regulator notification requirements	Any information holder that experiences a breach of system security must disclose to the attorney general by mail or electronic mail any breach of system security that **exceeds 250 residents** of this state. If an information holder discovers circumstances that require notification pursuant to § 22-40-20, the information holder must also notify, without unreasonable delay, all consumer reporting agencies, as defined under 15 U.S.C. § 1681a, in effect as of January 1, 2018, and any other credit bureau or agency that compiles and maintains files on consumers on a nationwide basis of the timing, distribution and content of the notice.
Enforcement	The attorney general may prosecute each failure to disclose under the provisions of §§ 22-40-19 to 22-40-26, inclusive, as a deceptive act or practice under § 37-24-6. In addition to any remedy provided under chapters 37-24, the attorney general may bring an action to recover on behalf of the state a civil penalty of not more than $10,000 per day per violation. The attorney general may recover attorney's fees and any costs associated with any action brought.

Tennessee

Statute (link)	Tenn. Code § 47-18-2107
What's a breach?	Breach of system security means the acquisition of the information by an unauthorized person who materially compromises the security, confidentiality or integrity of personal information maintained by the information holder. This information includes: • Unencrypted computerized data; or • Encrypted computerized data and the encryption key. A breach does not include the good faith acquisition of personal information by an employee or agent of the information holder for the purposes of the information holder if the personal information is not used or subject to further unauthorized disclosure.
What's considered personal information?	Personal information means an individual's first name or first initial and last name, in combination with one or more of the following data elements: • Social Security number; • Driver's license number; or • Account, credit card 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. Personal information does not include information that is lawfully made available to the general public from federal, state or local government records or information that has been redacted or otherwise made unusable.
Individual notification requirements	Following discovery or notification of a breach of system security by an information holder, the information holder must disclose the breach of system security to any resident of this state whose personal information was or is reasonably believed to have been acquired by an unauthorized person. The disclosure must be made no later than **45 days** from the discovery or notification of the breach of system security unless a longer period of time is required due to the legitimate needs of law enforcement. The required notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. If the notification is delayed, it must be made no later than **45 days** after the law enforcement agency determines that notification will not compromise the investigation.
Regulator notification requirements	If an information holder discovers circumstances requiring notification of **more than 1,000 persons** at one time, the information holder must also notify, without unreasonable delay, all consumer reporting agencies, as defined by 15 U.S.C. § 1681a, and credit bureaus that compile and maintain files on consumers on a nationwide basis of the timing, distribution and content of the notices.

Enforcement	Any customer of an information holder who is a person or business entity but who is not an agency of this state or any political subdivision of this state and who is injured by a violation of data breach notification requirements may institute a civil action to recover damages and to enjoin the information holder from further action in violation of data breach notification requirements. The rights and remedies available are cumulative to each other and to any other rights and remedies available under law.

Texas

Statute (link)	**Tex. Bus. & Com. Code §§ 521.002, 521.053**
What's a breach?	Breach of system security means 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. Good faith acquisition of sensitive personal information by an employee or agent of the person for the purposes of the person is not a breach of system security unless the person uses or discloses the sensitive personal information in an unauthorized manner.
What's considered personal information?	Personal identifying information means information that alone or in conjunction with other information identifies an individual, including an individual's: • Name, Social Security number, date of birth or government-issued identification number; • Mother's maiden name; • Unique biometric data, including the individual's fingerprint, voice print and retina or iris image; • Unique electronic identification number, address or routing code; and • Telecommunication access device as defined by Section 32.51, Penal Code.
Individual notification requirements	After discovering or receiving notification of the breach, a person who conducts business in this state and owns or licenses computerized data that includes sensitive personal information must disclose any breach of system security to any individual whose sensitive personal information was or is reasonably believed to have been acquired by an unauthorized person. The disclosure must be made without unreasonable delay and, in each case, no later than **the 60th day** after the date on which the person determines the breach occurred, unless an exception applies or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system. A person may delay providing the required notice at the request of a law enforcement agency that determines that the notification will impede a criminal investigation. The notification must be made as soon as the law enforcement agency determines that the notification will not compromise the investigation.
Regulator notification requirements	A person who is required to disclose or provide notification of a breach of system security must notify the attorney general of that breach no 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.

	The attorney general will post on the attorney general's publicly accessible Internet website a listing of the notifications received by the attorney general, excluding any sensitive personal information that may have been reported to the attorney general under that subsection, any information that may compromise a data system's security and any other information reported to the attorney general that is made confidential by law. 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 must also notify each consumer reporting agency, as defined by 15 U.S.C. Section 1681a, that maintains files on consumers on a nationwide basis of the timing, distribution and content of the notices. The person must provide the notice required by this subsection without unreasonable delay.
Enforcement	Remedies include injunctive relief and civil penalties of at least $2,000 but not more than $50,000 for each violation. Civil penalties for failure to comply with notification requirements are up to $100 per person to whom notification is due, per day, not to exceed $250,000 per breach.

Utah

Statute (link)	Utah Code §§ 13-44-101, 13-44-202, 13-44-301
What's a breach?	Breach of system security means unauthorized acquisition of computerized data maintained by a person who compromises the security, confidentiality or integrity of personal information. A breach of system security does not include the acquisition of personal information by an employee or agent of the person possessing unencrypted computerized data unless the personal information is used for an unlawful purpose or disclosed in an unauthorized manner.
What's considered personal information?	Personal information means a person's first name or first initial and last name, combined with 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: • Social Security number; • Financial account number or credit or debit card number; • Any required security code, access code or password that would permit access to the person's account; or • Driver license number or state identification card number. Personal information does not include information regardless of its source, contained in federal, state or local government records or in widely distributed media that are lawfully made available to the general public.
Individual notification requirements	A person who owns or licenses computerized data that includes personal information concerning a Utah resident must, when they becomes aware of a breach of system security, 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 must provide notification to each affected Utah resident. A person required to provide notification must provide the notification in the most expedient time possible without unreasonable delay: • While considering legitimate investigative needs of law enforcement; • After determining the scope of the breach of system security; and • After restoring the reasonable integrity of the system. A person may delay providing notification at the request of a law enforcement agency that determines that notification may impede a criminal investigation. A person who delays providing notification must

	provide notification in good faith without unreasonable delay in the most expedient time possible after the law enforcement agency informs the person notification will no longer impede the criminal investigation.
Regulator notification requirements	*No information on regulator notification requirements is available at this time.*
Enforcement	A person who violates data breach notification requirements is subject to a civil penalty of: ● Up to $2,500 for a violation or series of violations concerning a specific consumer; and ● Up to $100,000 in the aggregate for related violations concerning more than one consumer, unless the violations concern: ○ 10,000 or more consumers who are residents of the state; and ○ 10,000 or more consumers who are residents of other states; or ○ The person agrees to settle for a greater amount.

Vermont

Statute (link)	9 V.S.A. §§ 2430, 2435
What's a breach?	Security breach means unauthorized acquisition of electronic data or a reasonable belief of an unauthorized acquisition of electronic data that compromises the security, confidentiality or integrity of a consumer's personally identifiable information or login credentials maintained by a data collector. Security breach does not include good faith but unauthorized acquisition of personally identifiable information or login credentials by an employee or agent of the data collector for a legitimate purpose of the data collector, provided that the personally identifiable information or login credentials are not used for a purpose unrelated to the data collector's business or subject to further unauthorized disclosure.
What's considered personal information?	Personally identifiable information means a consumer's first name or first initial and last name in combination with one or more of the following digital data elements when the data elements are not encrypted, redacted or protected by another method that renders them unreadable or unusable by unauthorized persons: • A Social Security number; • A driver's 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; • A financial account number or credit or debit card number, if the number could be used without additional identifying information, access codes or passwords; • A password, personal identification number or other access code for a financial account; • Unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee of the data to identify or authenticate the consumer, such as a fingerprint, retina or iris image or other unique physical representation or digital representation of biometric data; • Genetic information; • Health records or records of a wellness program or similar program of health promotion or disease prevention; • A health care professional's medical diagnosis or treatment of the consumer; or • A health insurance policy number.

	Personally identifiable information does not include publicly available information that is lawfully made available to the general public from federal, state or local government records.
Individual notification requirements	Except as otherwise provided in subsection (d), any data collector that owns or licenses computerized personally identifiable information or login credentials must notify the consumer that there has been a security breach following discovery or notification to the data collector of the breach. Notice of the security breach must be made in the most expedient time possible and without unreasonable delay but no later than **45 days** after the discovery or notification, consistent with the legitimate needs of the law enforcement agency or with any measures necessary to determine the scope of the security breach and restore the reasonable integrity, security and confidentiality of the data system.
Regulator notification requirements	The data collector must notify the attorney general or the department, as applicable, of the date of the security breach and the date of discovery of the breach and must provide a preliminary description of the breach **within 14 business days**, consistent with the legitimate needs of the law enforcement agency of the data collector's discovery of the security breach or when the data collector provides notice to consumers, whichever is sooner. In the event a data collector provides notice to **more than 1,000 consumers** at one time, the data collector must notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. § 1681a(p), of the timing, distribution and content of the notice. This subsection must not apply to a person who is licensed or registered under Title 8 by the Department of Financial Regulation.
Enforcement	With respect to all data collectors and other entities subject to data breach notification requirements, other than a person or entity licensed or registered with the Department of Financial Regulation, the attorney general and state's attorney have sole and full authority to investigate potential violations of this subchapter and to enforce, prosecute, obtain and impose remedies for a violation of data breach notification requirements. The attorney general may refer the matter to the state's attorney in an appropriate case. The Superior Courts have jurisdiction over any enforcement matter brought by the attorney general or a state's attorney under this subsection. With respect to a data collector that is a person or entity licensed or registered with the Department of Financial Regulation, the Department of Financial Regulation has the full authority to investigate potential violations of this subchapter and to prosecute, obtain and impose remedies for a violation of data breach notification requirements.

Virginia

Statute (link)	**Va. Code § 18.2-186.6**
What's a breach?	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 the individual or entity reasonably believes has caused or will cause identity theft or other fraud to any resident of the Commonwealth. Good faith acquisition of personal information by an employee or agent of an individual or entity for the purposes of the individual or entity is not a breach of the security of the system, provided that the personal information is not used for a purpose other than a lawful purpose of the individual or entity or subject to further unauthorized disclosure.
What's considered personal information?	Personal information means the first name or first initial and last name in combination with and linked to one or more of the following data elements that relate to a Virginia resident when the data elements are neither encrypted nor redacted: • Social Security number; • Driver's license number or state identification card number issued in lieu of a driver's license number; • 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; • Passport number; or • Military identification number. Personal information does not include information that is lawfully obtained from publicly available information or from federal, state or local government records lawfully made available to the general public.
Individual notification requirements	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 Virginia resident, an individual or entity that owns or licenses computerized data that includes personal information must disclose any breach of the security of the system following discovery or notification of the breach of the security of the system any affected Virginia resident without unreasonable delay. Required notice 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. Required notice 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. Notice must be made without unreasonable delay after the law-enforcement agency determines that the notification will no longer impede the investigation or jeopardize national or homeland security.
Regulator notification requirements	In the event an individual or entity provides notice to **more than 1,000 persons** at one time, the individual or entity must notify, without unreasonable delay, the Office of the Attorney General and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. § 1681a (p), of the timing, distribution and content of the notice. 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 Virginia resident, an individual or entity that owns or licenses computerized data that includes personal information must disclose any breach of the security of the system following discovery or notification of the breach of the security of the system to the Office of the Attorney General without unreasonable delay.
Enforcement	The Office of the Attorney General may impose a civil penalty not to exceed $150,000 per breach of the security of the system or a series of breaches of a similar nature that are discovered in a single investigation. Nothing in this section limits an individual from recovering direct economic damages from a violation of data breach notification requirements.

Washington

Statute (link)	**Wash. Rev. Code § 19.255.010 et seq., § 42.56.590**
What's a breach?	Breach of the security of the system means unauthorized acquisition of data that compromises the security, confidentiality or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system when the personal information is not used or subject to further unauthorized disclosure.
What's considered personal information?	Personal information means an individual's first name or first initial and last name in combination with one or more of the following data elements: • Social Security number; • Driver's license number or Washington identification card number; • Account number or credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account or any other numbers or information that can be used to access a person's financial account; • Full date of birth; • Private key that is unique to an individual and that is used to authenticate or sign an electronic record; • Student, military or passport identification number; • Health insurance policy number or health insurance identification number; • Any information about a consumer's medical history or mental or physical condition or about a health care professional's medical diagnosis or treatment of the consumer; or • Biometric data generated by automatic measurements of an individual's biological characteristics such as a fingerprint, voiceprint, eye retinas, irises or other unique biological patterns or characteristics that is used to identify a specific individual; • Username or email address in combination with a password or security questions and answers that would permit access to an online account; and • Any of the data elements or any combination of the data elements above without the consumer's first name or first initial and last name if: ○ Encryption, redaction or other methods have not rendered the data element or combination of data elements unusable; and

	○ The data element or combination of data elements would enable a person to commit identity theft against a consumer. Personal information does not include publicly available information that is lawfully made available to the general public from federal, state or local government records.
Individual notification requirements	Any person or business that conducts business in this state and that owns or licenses data that includes personal information must disclose any breach of the security of the system to any resident of this state whose personal information was or is reasonably believed to have been acquired by an unauthorized person and the personal information was not secured. Notice is not required if the breach of the security of the system is not reasonably likely to subject consumers to a risk of harm. The breach of secured personal information must be disclosed if the information acquired and accessed is not secured during a security breach or if the confidential process, encryption key or other means to decipher the secured information was acquired by an unauthorized person. Notification to affected consumers must be made in the most expedient time possible, without unreasonable delay and no more than **30 calendar days** after the breach was discovered, unless the delay is at the request of law enforcement or the delay is due to any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. Required notification may be delayed if the data owner or licensee contacts a law enforcement agency after the discovery of a breach of the security of the system and a law enforcement agency determines that the notification will impede a criminal investigation. Required notification must be made after the law enforcement agency determines that it will not compromise the investigation.
Regulator notification requirements	Any person or business that is required to issue a notification to **more than 500 Washington residents** as a result of a single breach must notify the attorney general of the breach no more than 30 days after the breach was discovered.
Enforcement	The attorney general may bring action on behalf of the state or its residents. Violations of data breach notification requirements are unfair or deceptive acts and an unfair method of competition.

West Virginia

Statute (link)	W. VA. Code § 46A-2A-101 et seq.
What's a breach?	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 this state. Good faith acquisition of personal information by an employee or agent of an individual or entity for the purposes of the individual or the entity is not a breach of the security of the system, provided that the personal information is not used for a purpose other than a lawful purpose of the individual or entity or subject to further unauthorized disclosure.
What's considered personal information?	Personal information means the first name or first initial and last name linked to 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: • Social Security number; • Driver's license number or state identification card number issued in lieu of a driver's license; or • 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. Personal information does not include information that is lawfully obtained from publicly available information or from federal, state or local government records lawfully made available to the general public.
Individual notification requirements	An individual who or entity that owns or licenses computerized data that includes personal information must give notice of any breach of the security of the system following discovery or notification of the breach of the security of the system to any resident of this state 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 the individual or entity reasonably believes has caused or will cause identity theft or other fraud to any resident of this state. Notice must be made without unreasonable delay unless an entity is required to delay notice because of a law enforcement order or to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the system. An individual or entity must give notice of the breach of the security of the system if encrypted information is accessed and acquired in an

	unencrypted form or if the security breach involves a person with access to the encryption key and the individual or entity reasonably believes that such breach has caused or will cause identity theft or other fraud to any resident of this state. Required notice may be delayed if a 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. Similarly, the required notice must be made without unreasonable delay after the law enforcement agency determines that notification will no longer impede the investigation or jeopardize national or homeland security.
Regulator notification requirements	If an entity is required to notify **more than 1,000 persons** of a breach of security, the entity must also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on a nationwide basis, as defined by 15 U.S.C. §1681a (p), of the timing, distribution and content of the notices. Nothing in this obligation must be construed to require the entity to provide to the consumer reporting agency the names or other personal identifying information of breach notice recipients. This requirement does not apply to an entity that is subject to Title V of the Gramm Leach Bliley Act, 15 U.S.C. 6801, et seq.
Enforcement	The attorney general has exclusive authority to bring legal action for violations of data breach notification requirements. No civil penalty may be assessed in an action unless the court finds that the defendant has engaged in the course of repeated and willful violations its obligations. No civil penalty will 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. A violation of data breach notification requirements by a licensed financial institution is enforceable exclusively by the financial institution's primary functional regulator.

Wisconsin

Statute (link)	**Wis. Stat. § 134.98**
What's a breach?	A breach means a situation in which an entity that maintains or licenses personal information knows that the personal information in the entity's possession has been acquired by a person whom the entity has not authorized to acquire the personal information.
What's considered personal information?	Personal information means 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: • The individual's Social Security number; • The individual's driver's license number or state identification number; • 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; • The individual's DNA profile, as defined in s. 939.74 (2d) (a); or • The individual's unique biometric data, including fingerprint, voice print, retina or iris image or any other unique physical representation.
Individual notification requirements	When a breach takes place, an entity whose principal place of business is located in Wisconsin or an entity that maintains or licenses personal information in Wisconsin must make reasonable efforts to notify each subject of the personal information. Similarly, if an entity whose principal place of business is not located in Wisconsin knows that personal information pertaining to a resident of this state has been acquired by a person whom the entity has not authorized to acquire the personal information, the entity must make reasonable efforts to notify each resident of this state who is the subject of the personal information. The notice must indicate that the entity knows of the unauthorized acquisition of personal information pertaining to the resident of this state who is the subject of the personal information. The entity must provide the required notice within a reasonable time, not to exceed **45 days** after the entity learns of the acquisition of personal information. A determination as to reasonableness must include consideration of the number of notices that an entity must provide and the methods of communication available to the entity. An entity is not required to provide notice of the acquisition of personal information if any of the following applies:

	• The acquisition of personal information does not create a material risk of identity theft or fraud to the subject of the personal information; or • The personal information was acquired in good faith by an employee or agent of the entity, if the personal information is used for a lawful purpose of the entity. A law enforcement agency may, in order to protect an investigation or homeland security, ask an entity not to provide a notice that is otherwise required for any period of time, and the notification process required must begin at the end of that time period. If an entity receives such a request, the entity may not provide notice of or publicize an unauthorized acquisition of personal information, except as authorized by the law enforcement agency that made the request.
Regulator notification requirements	If, as the result of a single incident, an entity is required to notify **1,000 or more individuals** that personal information pertaining to the individuals has been acquired, the entity must without unreasonable delay notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 USC 1681a(p), of the timing, distribution and content of the notices sent to the individuals.
Enforcement	Whoever is concerned in the commission of a violation of this chapter for which forfeiture is imposed is a principal and may be charged with and convicted of the violation, although he or she did not directly commit it and although the person who directly committed it has not been convicted of the violation.

Wyoming

Statute (link)	Wyo. Stat. § 40-12-501 et seq.
What's a breach?	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 maintained by a person or business and causes or is reasonably believed to cause loss or injury to a resident of this state. Good faith acquisition of personal identifying information by an employee or agent of a person or business for the purposes of the person or business is not a breach of the security of the data system, provided that the personal identifying information is not used or subject to further unauthorized disclosure.
What's considered personal information?	Personal identifying information means the first name or first initial and last name of a person in combination with one or more of the following data elements: • Address; • Telephone number; • Social Security number; • Driver's license number; • Account number, credit card number or debit card number in combination with any security code, access code or password that would allow access to a financial account of the person; • Tribal identification card; • Federal or state government-issued identification card; • Shared secrets or security tokens that are known to be used for data-based authentication; • A username or email address, in combination with a password or security question and answer that would permit access to an online account; • A birth or marriage certificate; • Medical information, meaning a person's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; • Health insurance information, meaning a person's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the person or information related to a person's application and claims history; • Unique biometric data, meaning data generated from measurements or analysis of human body characteristics for authentication purposes; or • An individual taxpayer identification number.

	Personal identifying information does not include information, regardless of its source, contained in any federal, state or local government records or widely distributed media that are lawfully made available to the general public.
Individual notification requirements	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 must, when it becomes aware of a breach of the security of the system, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal identifying information has been or will be misused. If the investigation determines that the misuse of personal identifying information about a Wyoming resident has occurred or is reasonably likely to occur, the individual or the commercial entity must give notice as soon as possible to the affected Wyoming resident. Notice must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system. Required notification may be delayed if a law enforcement agency determines in writing that the notification may seriously impede a criminal investigation.
Regulator notification requirements	*No information regarding regulator notification requirements is available at this time.*
Enforcement	The attorney general may bring an action in law or equity to address any violation of this section and for other relief that may be appropriate to ensure proper compliance with this section, to recover damages or both. These provisions are not exclusive and do not relieve an individual or a commercial entity subject to this section from compliance with all other applicable provisions of the law.

This guide is not meant to be exhaustive or construed as legal advice. It does not address all potential compliance issues with federal/state/local government or any other regulatory agency standards. Consult legal counsel to address possible compliance requirements.