GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

The following definitions for General State Privacy Breach/Consumer Protection Laws have similar meanings in all the states unless otherwise noted.

Personal Information Defined (Encryption/Unencrypted)

"Personal information" means information that consists of a combination of an individual's first name or first initial and last name and one or more of the following data elements: the individual's SSN, driver's license number, or state identification card number; the individual's bank account number, credit card number, or debit card number; or passwords, personal identification numbers, or other access codes for financial accounts.

Breach of Security Defined

"Breach of the security", or "Breach of the security of the system", means unauthorized acquisition, or reasonable belief of unauthorized acquisition, of personal information that compromises the security, confidentiality, or integrity of the personal information maintained by an individual or commercial entity.

Good Faith Exception Defined

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 is not considered breach of security.

NOTE: The NAIC's Insurance Data Security Model Law (#668) was adopted in 2017. State provisions adopting #668 can be found here:
https://content.naic.org/sites/default/files/model-law-state-page-668.pdf

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

The date following each state indicates the last time information for the state was reviewed/changed.

	ALABAMA (8/23)
Citation	§§ 8-38-1 to 8-38-12
Person Covered	"Covered entity" means a person, sole proprietorship, partnership, government entity, corporation, nonprofit, trust, estate, cooperative association, or other business entity that acquires or uses sensitive personally identifying information. "Individual" means any Alabama resident whose sensitive personally identifying information was, or the covered entity reasonably believes to have been, accessed as a result of the breach.
Notification of Breach (Required)	A covered entity that is not a third-party agent, shall give notice of the breach to each individual. If the number of individuals a covered entity is required to notify exceeds 1,000, the entity shall provide written notice of the breach to the attorney general as expeditiously as possible and without unreasonable delay. If a covered entity discovers circumstances requiring notice of more than 1,000 individuals at a single time, the entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis. A third-party agent shall notify the covered entity of the breach of security as expeditiously as possible and without unreasonable delay, but no later than 10 days following the determination of the breach of security or reason to believe the breach occurred.
Notification of Breach (Delay/Exemption)	If a federal or state law enforcement agency determines that notice to individuals required under this section would interfere with a criminal investigation or national security, the notice shall be delayed upon the receipt of written request of the law enforcement agency for a period that the law enforcement agency determines is necessary.
Personal Information Defined (Encryption/Unencrypted)	"Sensitive personally identifying information" means an Alabama resident's first name or first initial and last name in combination with one or more delineated pieces of information.
Breach of Security Defined	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. Good faith exception.
Penalties	A covered entity that violates the notification provisions of this act shall 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 of this act. Civil penalties shall not exceed $500,000 per breach.
Private Cause of Action/Enforcement	A violation of this act does not establish a private cause of action.

ALABAMA (cont.)

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	ALABAMA (cont.)
Safeguards	Each covered entity and third-party agent shall implement and maintain reasonable security measures to protect sensitive personally identifying information against breach of security. A covered entity or third-party agent shall take reasonable measures to dispose, or arrange for the disposal, of records containing sensitive personally identifying information within its custody or control when the records are no longer to be retained pursuant to applicable law, regulations, or business needs. Disposal shall include shredding, erasing, or otherwise modifying the personal information in the records to make it unreadable or undecipherable through any reasonable means consistent with industry standards.
Other provisions	If a covered entity determines that notice is not required under this section, the entity shall document the determination in writing and maintain records concerning the determination for no less than 5 years.

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	ALASKA (8/23)
Citation	AS §§ 45.48.010 to 45.48.090; 45.48.510
Person Covered	Covered person means a person doing business; governmental agency; or person with more than 10 employees. "Information collector" means a covered person who owns or licenses personal information in any form if the personal information includes personal information on a state resident. "Information distributor" means a person who is an information collector and who owns or licenses personal information to an information recipient. "Information recipient" means a person who is an information collector but who does not own or have the right to license to another information collector the personal information received by the person from an information distributor.
Notification of Breach (Required)	Any covered person who owns or licenses personal information in any form must notify a state resident whose personal information was subject to a breach of the breach. An information collector shall provide notification in the most expeditious time possible and without unreasonable delay. An information collector that is required to notify more than 1,000 state residents of a breach, shall notify without unreasonable delay all consumer credit reporting agencies. An information recipient shall notify the information distributor of a breach immediately after the information recipient discovers the breach. Disclosure is not required if, after an appropriate investigation and after written notification to the attorney general, the covered person determines that there is not a reasonable likelihood that harm to the consumers whose personal information has been acquired has resulted or will result from the breach.
Notification of Breach (Delay/Exemption)	Notification may be delayed if law enforcement determines notification will impede a criminal investigation.
Personal Information Defined (Encryption/Unencrypted)	"Personal information" means 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.
Breach of Security Defined	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. Good faith exception.

ALASKA (cont.)

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	ALASKA (cont.)
Penalties	An information collector may be liable to the state for a civil penalty of up to $500 for each state resident who was not notified of the breach, but the total civil penalty may not exceed $50,000.
Private Cause of Action/Enforcement	No provision
Safeguards	The measures that may be taken to comply with AS § 45.48.500 include: implementing and monitoring compliance with policies and procedures that require the destruction or erasure of electronic media and other nonpaper media containing personal information so that the personal information cannot practicably be read or reconstructed.
Other provisions	Waiver is void and unenforceable.

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	ARIZONA (8/23)
Citation	§§ 18-551 to 18-552
Person Covered	A person that conducts business in this state and that owns, maintains or licenses unencrypted computerized data that includes personal information.
Notification of Breach (Required)	Any person that conducts business in this state and that owns, maintains or licenses unencrypted and unredacted computerized personal information shall, if there has been a breach, notify the individuals affected. The notice shall be made within 45 days after determination. Any person that maintains unencrypted and unredacted computerized personal information that the person does not own or license shall notify, as soon as practicable, the owner or licensee of the information on discovering any security system breach. If the breach requires notification of more than 1,000 individuals, must notify the three largest nationwide consumer reporting agencies, attorney general, and the director of the Arizona Department of Homeland Security.
Notification of Breach (Delay/Exemption)	Notification may be delayed if law enforcement determines notification will impede a criminal investigation.
Personal Information Defined (Encryption/Unencrypted)	"Personal information" means an individual's first name or first initial and last name in combination with one or more specified data elements; an individual's username or e-mail 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.
Breach of Security Defined	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. Good faith exception.
Penalties	The attorney general may impose a civil penalty for a violation of this article not to exceed the lesser of $10,000 per affected individual or the total amount of economic loss sustained by affected individuals, but the maximum civil penalty from a breach or series of related breaches may not exceed $500,000. This section does not prevent the attorney general from recovering restitution for affected individuals.

ARIZONA (cont.)

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	ARIZONA (cont.)
Private Cause of Action/Enforcement	No, may only be enforced by the attorney general.
Safeguards	The department of public safety, a county sheriff's department, a municipal police department, a prosecution agency and a court shall create and maintain an information security policy that includes notification procedures for a security system breach of the department of public safety, the county sheriff's department, the municipal police department, the prosecuting agency, or the court.
Other provisions	Does not apply to a person that is subject to title V of GLBA. Does not apply to covered entities or business associates subject to HIPAA regulation.

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	ARKANSAS (8/23)
Citation	§§ 4-110-101 to 4-110-108
Person Covered	Any person or business that acquires, owns, or licenses, or maintains computerized data that includes personal information.
Notification of Breach (Required)	A person or business that acquires, owns, or licenses computerized data that includes personal information shall notify any resident of Arkansas whose personal information is reasonably believed to have been acquired by an unauthorized person. The notification must be made in the most expedient time and manner possible without unreasonable delay. A person or business that maintains computerized data that includes personal information shall notify the owner or licensee of the information of any breach immediately following the discovery if the personal information is reasonably believed to have been acquired from an unauthorized person. If a breach of the security of a system affects the personal information of more than 1,000 individuals, the person or business shall disclose the security breach to the Attorney General.
Notification of Breach (Delay/Exemption)	Notification may be delayed if law enforcement determines notification will impede a criminal investigation. Notification is not required if, after a reasonable investigation, the person or business determines that there is no reasonable likelihood of harm to customers.
Personal Information Defined (Encrypted/Unencrypted)	"Personal information" means an individual's first name or first initial and the last name in combination with another identifying data element in any form on an individual when the name or the identifying data element is not encrypted or redacted. Personal information also includes medical information and biometric data.
Breach of Security Defined	Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person or business. Good faith exception.
Penalties	Violation is punishable by action of the attorney general under the provisions of the Deceptive Trade Practices Act, §§ 4-88-101 to 4-88-116.
Private Cause of Action/Enforcement	No, enforcement by attorney general only.
Safeguards	A person or business that acquires, owns, or licenses personal information about an Arkansas resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.
Other provisions	Bulletin No. 1-2006 (January 17, 2006) Any waiver of a provision of this chapter is contrary to public policy, void, and unenforceable.

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	CALIFORNIA (8/23)
Citation	Cal. Civ. Code §§ 1798.21; 1798.29; 1798.3; 1798.53 to 1798.57; 1798.81; 1798.81.5; 1798.82; 1798.84
Person Covered	Any person, agency or business that conducts business in California and owns, licenses, or maintains computerized data that includes personal information.
Notification of Breach (Required)	Any covered person shall disclose any breach of the security of the system following discovery or notification of the breach to any resident of California whose unencrypted personal information was or is reasonably believed to have been acquired by unauthorized persons. Any agency that maintains computerized data that includes personal information shall notify the owner or licensee of the information of any breach immediately following discovery if the personal information is reasonably believed to be acquired by an unauthorized person. Notice shall be made in the most expedient time possible and without unreasonable delay. Any agency required to issue a breach notification to more than 500 residents shall submit a copy of the breach notification to the attorney general.
Notification of Breach (Delay/Exemption)	Notification may be delayed if law enforcement determines notification will impede a criminal investigation.
Personal Information Defined (Encrypted/Unencrypted)	"Personal information" means any information that is maintained by an agency that identifies or describes an individual, including, but not limited to, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history. It includes statements made by, or attributed to, the individual. "Personal information" also includes an individual's first name or first initial and the individual's last name in combination with any one or more of the listed data elements, when either the name or the data elements are not encrypted. Data elements include medical information; health insurance information; and 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.
Breach of Security Defined	Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith exception.
Penalties	In any successful civil action brought under this section, the complainant, in addition to any special or general damages awarded, shall 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.

CALIFORNIA (cont.)

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	CALIFORNIA (cont.)
Private Cause of Action/Enforcement	Any customer injured by a violation of this title may institute a civil action to recover damages.
Safeguards	Each agency shall establish appropriate and reasonable administrative, technical, and physical safeguards to ensure compliance with the provisions of this chapter, to ensure the security and confidentiality of records, and to protect against anticipated threats or hazards to their security or integrity which could result in injury. A business shall take all reasonable steps to dispose, or arrange for the disposal, of customer records within its custody or control containing personal information when the records are no longer to be retained by the business by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means.
Other provisions	Notice No. 5-16-2014 (May 16, 2014) Any waiver of a provision of this title is contrary to public policy and is void and unenforceable.

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	COLORADO (8/23)
Citation	Colo. Rev. Stat. § 6-1-716
Person Covered	A covered entity that maintains, owns or licenses computerized data that includes personal information about a resident of Colorado.
Notification of Breach (Required)	A covered entity that maintains, owns or licenses computerized data that includes personal information shall give notice to the 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. If a covered entity that uses a third-party service to maintain computerized data that includes personal information, then the third-party service provider shall give notice to and cooperate with the covered entity in the event of a security breach that compromises such computerized data, including notifying the covered entity of the breach in the most expedient time possible and without unreasonable delay. If a covered entity is required to notify more than 1,000 residents, all consumer reporting agencies must be notified in the most expedient time possible and without unreasonable delay.
Notification of Breach (Delay/Exemption)	Notification may be delayed if law enforcement determines notification will impede a criminal investigation.
Personal Information Defined (Encryption/Unencrypted)	"Personal information" means a Colorado resident's first name or first initial and last name in combination with another identifying data element in any form on an individual that is not encrypted, redacted, or secured by any other method rendering the name or the element unreadable or unusable. The term "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government needs.
Breach of Security Defined	The unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a covered entity. Good faith exception.
Penalties	Attorney general may bring actions in law or equity to address violations of this section.
Private Cause of Action/Enforcement	No, enforcement by attorney general only.
Safeguards	No provision
Other provisions	Waiver of notification rights or responsibilities is void as against public policy.

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	CONNECTICUT (8/23)
Citation	§§ 36a-701b; 42-471; 42-472a; Bulletin IC-25 (August 18, 2010)
Person Covered	Any person, business, or agency that conducts business in this state, and who, in the ordinary course of such entity's business, owns, licenses, or maintains computerized data that includes personal information.
Notification of Breach (Required)	A covered person who, in the ordinary course of such person's business, owns, or licenses computerized data that includes personal information, shall notify the attorney general and any resident of the state whose information was reasonably believed to be breached. Notice shall be made without unreasonable delay, but not later than 60 days after discovery of the breach. Any person that maintains computerized data that includes personal information shall notify the owner or licensee of any breach if the personal information is reasonably believed to have been breached. All licensees and registrants of the Connecticut Insurance Department are required to notify the Commissioner in writing of any information security incident which affects residents within 5 days.
Notification of Breach (Delay/Exemption)	Notification shall be delayed for a reasonable period of time if law enforcement determines notification will impede a criminal investigation and such law enforcement agency has made a request that the notification be delayed.
Personal Information Defined (Encryption/Unencrypted)	"Personal information" means an individual's first name or first initial and last name in combination with another identifying data element. Personal information that has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable. "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.
Breach of Security Defined	Unauthorized access to/acquisition of electronic files, media, databases or computerized data, containing personal information that has not been secured by encryption or any other method or technology that renders the personal information unreadable or unusable.
Penalties	Department of Consumer Protection may conduct an administrative hearing and impose a civil penalty of not more than $5,000. Violations constitute an unfair trade practice and shall be enforced by the attorney general. Any penalties collected under § 42-471 shall be deposited into the privacy protection guaranty and enforcement account. Failure to comply with the requirements of § 36a-701b shall constitute an unfair trade practice.

CONNECTICUT (cont.)

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	CONNECTICUT (cont.)
Private Cause of Action/Enforcement	No, enforcement by attorney general or Department of Consumer Protection only.
Safeguards	Any person in possession of personal information of another person shall safeguard the data, computer files, and documents containing the information from misuse by third parties, and shall destroy, erase, or make unreadable such data, computer files, and documents prior to disposal.
Other provisions	

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	DELAWARE (8/23)
Citation	6 Del.C. §§ 12B-100 to 12B-104
Person Covered	Any person who conducts business in this state and who owns or licenses computerized data that includes personal information, or a person that maintains computerized data that includes personal information that the person does not own or license. This includes persons regulated by state or federal law, including HIPAA.
Notification of Breach (Required)	A covered entity shall notify an affected Delaware resident as soon as possible of any breach if a misuse of personal information is reasonably likely to occur. Notice must be made in the most expedient time possible and without unreasonable delay, but not later than 60 days after determination of the breach of security or a shorter time if required by federal law. An individual or commercial entity that maintains computerized data that includes personal information shall notify the owner or licensee of any breach immediately following discovery if misuse of personal information is reasonably likely to occur. If the affected number of Delaware residents to be notified exceeds 500 residents, the person required to provide notice shall, not later than the time when notice is provided to the resident, also provide notice of the breach of security to the attorney general. If the breach includes a resident's social security number, the person shall provide credit monitoring services to the resident at no cost for a period of one year.
Notification of Breach (Delay/Exemption)	Notification may be delayed if law enforcement determines notification will impede a criminal investigation and such law-enforcement agency has made a request of the person that the notice be delayed.
Personal Information Defined (Encrypted/Unencrypted)	"Personal information" means a resident's first name or first initial and last name in combination with another identifying element. "Personal information" means 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. "Personal information" shall not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.
Breach of Security Defined	The unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information. Good faith exception.

DELAWARE (cont.)

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	DELAWARE (cont.)
Penalties	Attorney general may bring an action in law or equity to address violations of this chapter.
Private Cause of Action/Enforcement	Private right of action allowed.
Safeguards	Any person who conducts business in Delaware and owns, licenses, or maintains personal information shall maintain procedures and practice to prevent the unauthorized use of personal information.
Other provisions	Notice No. 10-16-2000 (October 16, 2000); Memorandum No. 11-21-2000 (November 21, 2000)

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	DISTRICT OF COLUMBIA (8/23)
Citation	§§ 28-3851 to 28-3853
Person Covered	Any person or entity who conducts business in the District of Columbia, and who, in the course of such business, owns, or licenses computerized or other electronic data that includes personal information and who discovers a breach of the security of the system; and any person or entity who maintains, handles or otherwise possesses computerized or other electronic data that includes personal information that the person or entity does not own and who discovers a breach of the security of the system.
Notification of Breach (Required)	Any covered person who owns or licenses computerized data that includes personal information shall notify of a breach any resident whose information was included in the breach. Notification shall be made at the most expedient time possible and without unreasonable delay. Written notice of the breach must be supplied to the attorney general if the breach affects 50 or more District residents. Any person or entity who maintains, handles, or otherwise possesses computerized personal information shall notify the owner or licensee of any breach in the most expedient time possible following discovery. If any person or entity is required to notify more than 1,000 persons, then all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis must be notified without unreasonable delay.
Notification of Breach (Delay/Exemption)	Notification may be delayed if law enforcement determines notification will impede a criminal investigation.
Personal Information Defined (Encryption/Unencrypted)	"Personal information" includes an individual's first name or initial and last name, or any other personal identifier combined with the other listed data elements. "Personal information" shall not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.
Breach of Security Defined	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 who conducts business in the District of Columbia. Good faith exception. "Breach of security" does not include acquisition of data that has been rendered secure, including through encryption or redaction of such data, so as 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.
Penalties	Violation of this chapter is an unfair and deceptive trade practice pursuant to § 28-3904(kk). Any person who requires notification of breach of their information must be offered identity theft protection for a period of not less than 18 months by the entity involved in the breach.

DISTRICT OF COLUMBIA (cont.)

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	DISTRICT OF COLUMBIA (cont.)
Private Cause of Action/Enforcement	No provision
Safeguards	A person or entity that owns, licenses, maintains, handles, or otherwise possesses personal information of an individual residing in the District shall implement and maintain reasonable security safeguards, including procedures and practices that are appropriate to the nature of the personal information and the nature and size of the entity or operation. When a person or entity is destroying records, the person or entity shall take reasonable steps to protect against unauthorized access to or use of the personal information.
Other provisions	Bulletin 00-003-LG (November 17, 2000) A waiver of any provision of this subchapter shall be void and unenforceable.

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	FLORIDA (8/23)
Citation	Fla. Stat. § 501.171
Person Covered	"Covered entity" means a sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity that acquires, maintains, stores, or uses personal information. For purposes of the notice requirements in subsections the term includes a governmental entity. "Third-party agent" means an entity that has been contracted to maintain, store, or process personal information on behalf of a covered entity or governmental entity.
Notification of Breach (Required)	A covered entity shall provide notice to the department if the breach affects 500 or more individuals, and to each affected individual whose personal information is reasonably believed to have been accessed. Notice must be provided as expeditiously as practicable and without unreasonable delay, 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 good cause for delay is provided. If a covered entity is required to provide notice to more than 1,000 individuals, notice must be given to all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis without unreasonable delay. Third parties maintaining a security system must notify the covered entity of any breach as expeditiously as practicable, but not later than 10 days following the determination of the breach or reason to believe the breach occurred.
Notification of Breach (Delay/Exemption)	Notification may be delayed upon a request by law enforcement if law enforcement determines notification will impede a criminal investigation.
Personal Information Defined (Encrypted/Unencrypted)	“Personal information” means an individual’s first name or first initial and last name in combination with any one or more data elements. It also includes a username or e-mail 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 government entity, and 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.
Breach of Security Defined	The unauthorized access of data in electronic form including personal information. Good faith exception.
Penalties	A violation of this section shall be treated as an unfair or deceptive trade practice. A covered entity that violates this section shall be liable for a civil penalty not to exceed $500,000.

FLORIDA (cont.)

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	FLORIDA (cont.)
Private Cause of Action/Enforcement	No private cause of action.
Safeguards	Each covered entity, governmental entity, or third-party agent shall take reasonable measures to protect and secure data in electronic form containing personal information.
Other provisions	

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	GEORGIA (8/23)
Citation	§§ 10-1-910 to 10-1-912
Person Covered	"Data collector" means any state or local agency or subdivision thereof including any department, bureau, authority, public university or college, academy, commission, or other government entity; provided, however, that the term "data collector" shall not include any governmental agency whose records are maintained primarily for traffic safety, law enforcement, or licensing purposes or for purposes of providing public access to court records or to real or personal property information. "Information broker" means any person or entity who, for monetary fees or dues, engages in whole or in part in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring, or communicating information concerning individuals for the primary purpose of furnishing personal information to nonaffiliated third parties, but does not include any governmental agency whose records are maintained primarily for traffic safety, law enforcement, or licensing purposes.
Notification of Breach (Required)	Any information broker or data collector that maintains computerized data that includes personal information of individuals shall give notice of any breach of the security of the system. Notice shall be made in the most expedient time possible without unreasonable delay. The information broker or data collector must be notified within 24 hours following discovery of the breach. Any covered person shall also notify, without unreasonable delay, all consumer reporting agencies in the event that the entity must notify more than 10,000 persons at one time.
Notification of Breach (Delay/Exemption)	Notification may be delayed if law enforcement determines notification will impede a criminal investigation.
Personal Information Defined (Encryption/Unencrypted)	"Personal information" means an individual's first name or first initial and last name in combination with the data elements when information is not encrypted or redacted. The term "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.
Breach of Security Defined	The 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 exception.
Penalties	No provision
Private Cause of Action/Enforcement	No provision
Safeguards	No provision
Other provisions	

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	GUAM (8/23)
Citation	9 G.C.A. §§ 48.10 to 48.80
Person Covered	An individual or entity that owns or licenses computerized data that includes personal information. An individual or entity that maintains computerized data that includes personal information that the individual or entity does not own or license.
Notification of Breach (Required)	An individual or entity that owns or licenses computerized data that includes personal information shall disclose any breach to any resident whose personal information is reasonably believed to have been acquired by an unauthorized person. Disclosure shall be made without unreasonable delay. An individual or entity that maintains computerized data that includes personal information shall notify the owner or licensee of the information of any breach as soon as practicable following discovery.
Notification of Breach (Delay/Exemption)	Notification may be delayed if law enforcement believes notification will impede a criminal investigation.
Personal Information Defined (Encrypted/Unencrypted)	"Personal information" is first name or initial, and last name in combination with one or more of the listed data elements. The data elements are neither encrypted nor redacted. "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.
Breach of Security Defined	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, identify theft or other fraud to any resident of Guam. Good faith exception.
Penalties	Attorney general may bring action to obtain damages 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.
Private Cause of Action/Enforcement	No, enforcement by attorney general only.
Safeguards	Public and private entities have a duty to safeguard personal information that, if stolen or publicized, may result in crimes such as fraud and identity theft. It is incumbent upon all entities that are entrusted with such data to maintain strong security systems to ensure that the personal information will always be protected.
Other provisions	

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	HAWAII (8/23)
Citation	H.R.S. §§ 487N-1 to 487N-7
Person Covered	Any business or government agency 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 or any government agency that collects personal information for specific government purposes and any business located in Hawaii or any business that conducts business in Hawaii that maintains or possesses records or data containing personal information of residents of Hawaii that the business does not own or license, or any government agency that maintains or possesses records or data containing personal information of residents of Hawaii.
Notification of Breach (Required)	Any business that owns or licenses personal or any government agency that collects personal information shall provide notice to the affected person that there has been a breach. The disclosure notification shall be made without unreasonable delay. Any business or government agency that maintains or possesses records or data containing personal information shall notify the owner or licensee of any breach immediately after discovery. A government agency shall submit a written report to the legislature within 20 days after discovery of a security breach at the government agency that details information relating to the nature of the breach, the number of individuals affected by the breach, a copy of the notice of security breach that was issued. Any business that is required to notify more than 1,000 persons must notify the office of consumer protection and all consumer reporting agencies that maintain files on consumers on a nationwide basis without unreasonable delay.
Notification of Breach (Delay/Exemption)	Notification shall be delayed if law enforcement agency informs the business or government agency that notification will impede a criminal investigation or jeopardize national security.
Personal Information Defined (Encrypted/Unencrypted)	“Personal information” means an individual’s first name or first initial and last name in combination with another identifying data element when either the name or the data elements are not encrypted. "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.
Breach of Security Defined	Good faith exception. 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.

HAWAII (cont.)

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	HAWAII (cont.)
Penalties	Any business that violates any provision of this chapter shall be subject to penalties of not more than $2,500 for each violation. In addition, any business that violates any provision of this chapter shall 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.
Private Cause of Action/Enforcement	No, the attorney general or the executive director of the office of consumer protection may bring an action pursuant to this section. No such action may be brought against a government agency.
Safeguards	No provision
Other provisions	Any waiver of the provisions of this section is contrary to public policy and is void and unenforceable.

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	IDAHO (8/23)
Citation	§§ 28-51-104 to 28-51-107
Person Covered	A city, county or state agency, individual or a commercial entity that conducts business in Idaho and that owns or licenses computerized data that includes personal information about a resident of Idaho and an agency, individual or a commercial entity that maintains computerized data that includes personal information that the agency, individual or the commercial entity does not own or license.
Notification of Breach (Required)	A covered entity that owns or licenses computerized data that includes personal information must, within 24 hours of becoming aware of a breach, notify, as soon as possible, the office of the Idaho Attorney General and the affected Idaho resident if a misuse of information is reasonably likely to occur. Notice must be made in the most expedient time possible and without unreasonable delay. A covered entity that maintains computerized data that includes personal information shall notify the owner or licensee of any breach immediately following discovery if misuse of the information is reasonably likely to occur.
Notification of Breach (Delay/Exemption)	Notification may be delayed if law enforcement determines notification will impede a criminal investigation.
Personal Information Defined (Encrypted/Unencrypted)	"Personal information" means first name or initial and last name, in combination with another identifying data element, when either the name or the data elements are not encrypted. "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.
Breach of Security Defined	The illegal acquisition of unencrypted computerized data that materially compromises the security, confidentiality, or integrity of personal information for one (1) or more persons maintained by an agency, individual or a commercial entity. Good faith exception.
Penalties	A covered entity in violation of this chapter shall be subject to a fine of not more than $25,000 per breach of the security system.
Private Cause of Action/Enforcement	No, enforcement by agency, individual or commercial entity's primary regulator only.
Safeguards	No provision
Other provisions	

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	ILLINOIS (8/23)
Citation	815 ILCS 530/1 to 530/50
Person Covered	"Data collector" may include, but is not limited to, government agencies, public and private universities, privately and publicly held corporations, financial institutions, retail operators, and any other entity that, for any purpose, handles, collects, disseminates, or otherwise deals with nonpublic personal information. Any data collector that owns or licenses personal information concerning an Illinois resident and any data collector that maintains or stores, but does not own or license, computerized data that includes personal information that the data collector does not own or license. Any state agency that collects personal information concerning an Illinois resident.
Notification of Breach (Required)	Any data collector that owns or licenses personal information shall notify, at no charge, the affected persons of a following discovery of a breach. Notice shall be made in the most expedient time possible and without unreasonable delay. Any data collector that maintains or stores computerized data that includes personal information shall notify the owner or licensee of any breach immediately following discovery if personal information is reasonably believed to be acquired by an unauthorized person. Any state agency that collects personal information shall notify the resident that there has been a breach of security. The notice shall be made in the most expedient time possible and without unreasonable delay. If the state agency is required to notify more than 1,000 persons at one time, the state agency shall also notify all consumer agencies that maintain files on consumers on a nationwide basis. Any data collector required to issue notice to more than 500 Illinois residents as a result of a single breach shall provide notice to the attorney general.
Notification of Breach (Delay/Exemption)	Notification may be delayed if law enforcement determines notification will impede a criminal investigation.
Personal Information Defined (Encryption/Unencrypted)	"Personal information" means first name or initial and last name, in combination with one or more data elements that are not encrypted or redacted or that are encrypted, and the encryption key has been acquired without authorization. "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.
Breach of Security Defined	The unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the data collector. Good faith exception.

ILLINOIS (cont.)

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	ILLINOIS (cont.)
Penalties	A violation of this act constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act. Any person who violates 530/40 is subject to a civil penalty of not more than $100 for each individual. A civil penalty may not exceed $50,000 for each instance of improper disposal of materials.
Private Cause of Action/Enforcement	No, but the attorney general may bring an action in the circuit court to remedy a violation of this section, seeking any appropriate relief.
Safeguards	A data collector that owns or licenses or maintains or stores but does not own or license, records that contain personal information concerning an Illinois resident shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure. Any state agency that collects personal data that is no longer needed or stored at the agency shall dispose of the personal data or written material it has collected in such a manner as to ensure the security and confidentiality of the material. Electronic media and other non-paper media containing personal information may be destroyed or erased so that the personal information cannot be read or reconstructed.
Other provisions	Any waiver of the provisions of this act is contrary to public policy and is void and unenforceable.

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	INDIANA (8/23)
Citation	IC 24-4.9-1-1 to 24-4.9-5-1; 4-1-11-1 to 4-1-11-10
Person Covered	Any person, entity, or state agency that owns or licenses computerized data that includes personal information. "Data base owner" means a person that owns or licenses computerized data that includes personal information.
Notification of Breach (Required)	Any covered person shall notify the affected resident whose unencrypted personal information or encrypted personal information with access to the encryption key may have been acquired by an unauthorized person. Disclosure shall be made without unreasonable delay, but no more than 45 days after discovery of breach. A database owner shall disclose the breach to an Indiana resident whose information was or may have been acquired by an unauthorized person. If disclosure is to more than 1,000 consumers, shall also disclose to each consumer reporting agency 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. A database owner shall also disclose a breach to the attorney general. Any state agency that owns or licenses computerized data that includes personal information shall, without delay, disclose a breach of the security of the system following discovery or notification of the breach to any state resident whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. If a state agency is required to provide notice to more than 1,000 persons, the state agency shall notify without unreasonable delay all consumer reporting agencies.
Notification of Breach (Delay/Exemption)	Notification may be delayed if a law enforcement agency or attorney general determines that the notification will impede a criminal investigation or jeopardize national security. Delay is also permissible if it is necessary to restore the integrity of the computer system or necessary to discover the scope of the breach.
Personal Information Defined (Encryption/Unencrypted)	"Personal information" means a social security number that is not encrypted or redacted; or an individual's first name or initial and last name in combination with another identifying data element that are not encrypted or redacted. "Personal information" does not include information that is lawfully made available to the public from records of a federal, state, or local government.
Breach of Security Defined	The unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person or a state or local agency. Good faith exception. "Breach of security" does not include unauthorized acquisition of a portable electronic device on which personal information is stored if all personal information is encrypted.

INDIANA (cont.)

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	INDIANA (cont.)
Penalties	For failure to make required disclosure or notification with regard to breaches, the attorney general may bring an action under this section to obtain a civil penalty of not more than $150,000 per deceptive act, and reasonable investigation costs. For failure to maintain safeguard procedures, attorney general may seek injunction, $5,000 per deceptive act, and reasonable investigation costs.
Private Cause of Action/Enforcement	No private cause of action.
Safeguards	A data base owner shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect and safeguard from unlawful use or disclosure any personal information of Indiana residents collected or maintained by the data base owner.
Other provisions	This section does not apply to a data base owner that maintains its own data security procedures as part of an information privacy, security policy, or compliance plan under: the U.S.A. Patriot Act; Executive Order 13224; Driver's Privacy Protection Act; Fair Credit Reporting Act; Financial Modernization Act of 1999; or HIPAA.

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	IOWA (8/23)
Citation	I.C.A. §§ 715C.1; 715C.2
Person Covered	Any person who owns or licenses or maintains computerized data that includes a consumer's personal information that is used in the course of the person's business, vocation, occupation, or volunteer activities.
Notification of Breach (Required)	Any person who owns or licenses computerized data that includes a consumer's personal information that was subject to a breach of security shall give notice of the breach to any consumer whose personal information was included in the breach. The consumer notification shall be made in the most expeditious manner possible and without unreasonable delay. Any person who maintains or possesses personal information shall notify the owner or licensee of the information of any breach immediately following discovery if a consumer's personal information was included in the breach. If notification is required to be sent out to more than 500 residents, the director of the consumer protection division of the office of the attorney general must be given notice within 5 days of the breach of security.
Notification of Breach (Delay/Exemption)	Notification may be delayed if law enforcement determines notification will impede a criminal investigation.
Personal Information Defined (Encryption/Unencrypted)	The data elements are not encrypted, redacted, or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable or are encrypted, redacted, or otherwise altered by any method or technology but the keys to unencrypt, unredact, or otherwise read the data elements have been obtained through the breach of security. "Personal information" means an individual's first name or initial and last name and another identifying piece of information. Personal information also includes: 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.
Breach of Security Defined	The unauthorized acquisition of personal information maintained in computerized form by a person that compromises the security, confidentiality, or integrity of the personal information. Good faith exception.
Penalties	A violation of this chapter is an unlawful practice under section 714.16. 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.
Private Cause of Action/Enforcement	No, enforcement by attorney general only.
Safeguards	No provision
Other provisions	

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	KANSAS (8/23)
Citation	K.S.A. 50-7a01 to 50-7a02; 50-7a04; 50-6,139b
Person Covered	A person that conducts business in this state, or a government, governmental subdivision or agency that owns or licenses computerized data that includes personal information and an individual or a commercial entity that maintains computerized data that includes personal information that the individual or the commercial entity does not own or license.
Notification of Breach (Required)	A covered person that owns or licenses computerized data that includes personal information shall notify the Kansas resident affected by any breach as soon as possible if misuse of information is reasonably likely to occur. Notice must be made in the most expedient time possible and without reasonable delay. A covered person that maintains computerized data must notify the owner or licensee of any breach following discovery if personal information is reasonably likely to have been acquired by an unauthorized person. A covered entity that is required to provide notice to more than 1,000 consumers shall notify, without unreasonable delay, all consumer reporting agencies that maintain files on consumers on a nationwide basis.
Notification of Breach (Delay/Exemption)	Notification may be delayed if law enforcement determines notification will impede a criminal investigation.
Personal Information Defined (Encryption/Unencrypted)	"Personal information" means first name or initial and last name and another piece of identifying information in any form on an individual that is not encrypted or redacted, and any other information which identifies an individual for which an information security obligation is imposed by federal or state statute or regulation. "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state or local government records.
Breach of Security Defined	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 exception.
Penalties	Each violation shall be an unconscionable act or practice in violation of K.S.A. 50-627. Each record not destroyed in compliance shall constitute a separate unconscionable act within the meaning of K.S.A. 50-627.
Private Cause of Action/Enforcement	No, for violations of this section by an insurance company licensed to do business in this state, the insurance commissioner shall have the sole authority to enforce the provisions of this section. The attorney general is empowered to bring an action in law or equity to address violations of this section and for other relief that may be appropriate.

KANSAS (cont.)

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	KANSAS (cont.)
Safeguards	A person or business shall take reasonable steps to destroy or arrange for the destruction of a customer's records within its custody or control containing personal information which is no longer to be retained by the person or business by shredding, erasing, or otherwise modifying the personal information in the records to make it unreadable or undecipherable through any means.
Other provisions	A holder of personal information shall have an affirmative defense to a violation if such holder proves by clear and convincing evidence that the security failure could not reasonably have been foreseen despite the holder's exercise of reasonable care; the holder of personal information had in effect at the time of the violation a bona fide written or electronic records management policy, including practices and procedures reasonably designed to prevent a violation.

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	KENTUCKY (8/23)
Citation	§§ 365.720; 365.725; 365.730; 365.732
Person Covered	"Information holder" means any person or business entity that conducts business in this state. Any information holder that maintains computerized data that includes personally identifiable information that the information holder does not own the information.
Notification of Breach (Required)	Any information holder shall disclose any breach to any Kentucky resident whose unencrypted personal information is reasonably believed to have been acquired by an unauthorized person. Notification must be made in the most expedient time possible and without unreasonable delay. Any information holder that maintains computerized data that includes personal information shall notify the owner or licensee of any breach as soon as reasonably practicable following discovery if personal information is reasonably believed to have been acquired by an unauthorized person. If a covered person must notify more than 1,000 persons at one time, all consumer reporting agencies and credit bureaus that maintain files on consumers on a nationwide basis shall be notified without unreasonable delay.
Notification of Breach (Delay/Exemption)	Notification may be delayed if law enforcement determines notification will impede a criminal investigation.
Personal Information Defined (Encryption/Unencrypted)	"Personally identifiable information" means information capable of being associated with a particular customer through one or more identifiers including the first name or first initial and one other identifiable data element that is not redacted.
Breach of Security Defined	The unauthorized acquisition of unencrypted or 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 KY resident. Good faith exception.
Penalties	No provision
Private Cause of Action/Enforcement	Any customer injured by a violation of § 365.725 may institute a civil action to recover damages.
Safeguards	When a business disposes of any customer's records, the business shall take reasonable steps to destroy that portion of the records containing personally identifiable information by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable or indecipherable through any means.
Other provisions	

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	LOUISIANA (8/23)
Citation	LSA-R.S. 51:3071 to 51:3077; LAC tit. 16, pt. III, § 701
Person Covered	Any person that conducts business in the state or that owns or licenses computerized data that includes personal information, or any agency that owns or licenses computerized data that includes personal information and any agency or person that maintains computerized data that includes personal information that the agency or person does not own.
Notification of Breach (Required)	Any covered person that owns or licenses computerized data that includes personal information shall, notify any resident of the state whose personal information is reasonably believed to have been acquired by an unauthorized person. Any covered person that maintains computerized data that includes personal information shall notify the owner or licensee of any breach if personal information is reasonably believed to have been acquired by an unauthorized person. The notification shall be made in the most expedient time possible and without unreasonable delay, but not later than 60 days from the discovery of the breach. When notice is required, the covered person shall provide notice to the Consumer Protection Section of the Attorney General's Office within 10 days of distribution of notice to the citizens of Louisiana.
Notification of Breach (Delay/Exemption)	Notification may be delayed if law enforcement determines notification will impede a criminal investigation.
Personal Information Defined (Encryption/Unencrypted)	"Personal information" means the first name or initial and the last name of an individual resident of the state and one other identifying element of information in any form on an individual that is not encrypted or redacted. "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.
Breach of Security Defined	The compromise of the security, confidentiality, or integrity of computerized data that results in, or there is a reasonable likelihood to result in, the unauthorized acquisition of and access to personal information maintained by an agency or person. Good faith exception.
Penalties	Failure to provide a timely notice may be punishable by a fine not to exceed $5,000 per violation.
Private Cause of Action/Enforcement	A violation of a provision of this chapter shall constitute an unfair act or practice pursuant to R.S. 51:1405(A). A civil action may be instituted to recover actual damages resulting from a failure to provide notice in a timely manner.
Safeguards	Any person that conducts business in the state or that owns or licenses computerized data that includes personal information, or any agency that owns or licenses computerized data that includes personal information shall take all reasonable steps to destroy or arrange for the destruction of the records within its custody or control containing personal information that is no longer to be retained by the person or business by shredding, erasing, or otherwise modifying the personal information in the records to make it unreadable or undecipherable through any means.
Other provisions	

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	MAINE (8/23)
Citation	10 Me. Rev. Stat. §§ 1346 to 1350-B
Person Covered	Person who maintains computerized data that includes personal information. "Information broker" means a person who, for monetary fees or dues, engages in whole or in part in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring or communicating information concerning individuals for the primary purpose of furnishing personal information to nonaffiliated third parties. "Information broker" does not include a governmental agency whose records are maintained primarily for traffic safety, law enforcement or licensing purposes.
Notification of Breach (Required)	An information broker or any other person that maintains computerized data that includes personal information shall give notice of a breach to a resident of this state whose personal information is reasonably believed to have been acquired by an unauthorized person or is reasonably believed to be misused. If there is no delay of notification due to law enforcement investigation, notices must be made no more than 30 days after awareness of the breach of security. A third-party entity that maintains computerized data that includes personal information shall notify the person maintaining the information of a breach immediately following discovery if personal information is reasonably believed to have been acquired by an unauthorized person. If a person is required to notify more than 1,000 residents, the person shall notify all consumer reporting agencies that maintain files on consumers on a nationwide basis without unreasonable delay. The information broker or any other person that maintains computerized data that includes personal information shall notify the appropriate state regulators in the department of professional and financial regulation or the attorney general when notice is required to be sent out.
Notification of Breach (Delay/Exemption)	Notification required by this section may be delayed for no longer than 7 business days after a law enforcement agency determines that the notification will not compromise a criminal investigation.
Personal Information Defined (Encrypted/Unencrypted)	"Personal information" means an individual's first name or initial and last name in combination with another identifiable data element and is information in any form on an individual that is not encrypted or redacted. "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.
Breach of Security Defined	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 exception.

MAINE (cont.)

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	MAINE (cont.)
Penalties	A fine of not more than $500 per violation, up to a maximum of $2,500 for each day the person is in violation of this chapter.
Private Cause of Action/Enforcement	No, enforcement by the department of professional and financial regulation or the attorney general.
Safeguards	No provision
Other provisions	Bulletin 345

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	MARYLAND (8/23)
Citation	§§ 14-3501 to 14-3508
Person Covered	A business that owns or licenses computerized data that includes personal information of an individual residing in the state and a business that maintains computerized data that includes personal information that the business does not own or license.
Notification of Breach (Required)	A covered person that owns or licenses computerized data that includes personal information shall notify the affected individuals of any breach if misuse of personal information is reasonably likely to occur. Notification shall be given as soon as reasonably practicable, but not later than 45 days after the business discovers or is notified of the breach. A covered person that maintains computerized data that includes personal information shall notify the owner or licensee of any breach if it is likely to cause the misuse of personal information. A business shall provide notice to the office of the attorney general. If a business is required to notify 1,000 or more persons, the business shall also notify, without unreasonable delay, each consumer reporting agency that maintains files on consumers on a nationwide basis.
Notification of Breach (Delay/Exemption)	Notification may be delayed if law enforcement determines notification will impede a criminal investigation or jeopardize homeland or national security; or to determine the scope of the breach, identify the individuals affected, or restore the integrity of the system.
Personal Information Defined (Encryption/Unencrypted)	"Personal information" means an individual's first name or initial and last name in combination with one or more identifying elements when not encrypted, redacted, or otherwise protected by another method that renders the information unreadable or unusable. It also includes 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; information that an individual has consented to have publicly disseminated or listed; or information that is disseminated or listed in accordance with the federal HIPAA.
Breach of Security Defined	The unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of the personal information maintained by a business. Good faith exception.
Penalties	A violation of this subtitle is an unfair or deceptive trade practice within the meaning of Title 13 of the Maryland Code.
Private Cause of Action/Enforcement	Yes, may bring action under the Unfair and Deceptive Trade Practices Act.
Safeguards	To protect personal information from unauthorized access, use, modification, or disclosure, a business that owns, maintains, or licenses personal information of an individual residing in the state shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal information owned, maintained, or licensed and the nature and size of the business and its operations.
Other provisions	Investigation records maintained for 3 years.

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	MASSACHUSETTS (8/23)
Citation	M.G.L.A. 93H §§ 1 to 6; 93A § 4
Person Covered	A person or agency that owns or licenses data, or any entity that maintains or stores, but does not own or license data that includes personal information about a resident of the commonwealth.
Notification of Breach (Required)	A person or agency that maintains or stores data that includes personal information shall notify the owner or licensor as soon as practicable and without unreasonable delay if the person or agency has reason to know of a breach of security or that personal information was acquired or used by an unauthorized person. A person or agency that owns or licenses data that includes personal information shall notify the attorney general, director of consumer affairs and business regulation, and to each affected resident as soon as practicable and without unreasonable delay if the person or agency has reason to know of a breach or that personal information was acquired or used by any unauthorized person. The director of consumer affairs and business regulation shall notify any relevant consumer reporting agency or state agency. If there is a breach of security that includes a social security number, credit monitoring services must be provided at no cost to resident for a period of not less than 18 months. If the agency is within the executive department, it shall notify the information technology division and the division of public records as soon as practicable and without unreasonable delay following discovery of a breach of unauthorized acquisition or use.
Notification of Breach (Delay/Exemption)	Notification may be delayed if law enforcement determines notification will impede a criminal investigation and has notified the attorney general in writing.
Personal Information Defined (Encryption/Unencrypted)	"Personal information" includes a resident's first name or initial and the last name in combination with another identifying data element but 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.
Breach of Security Defined	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. Good faith exception.

MASSACHUSETTS (cont.)

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	MASSACHUSETTS (cont.)
Penalties	Attorney general may bring an action pursuant to 93A § 4 to remedy violations of this chapter. Court may issue injunctions, require person to pay the commonwealth a civil penalty of not more than $5,000 for each violation, and require the person to pay reasonable costs of investigation and litigation, including reasonable attorneys' fees. Any person who violates the terms of an injunction or other order issued under this section shall pay to the commonwealth a civil penalty of not more than $10,000 for each violation.
Private Cause of Action/Enforcement	Maybe. If the court finds any violation of the commonwealth's consumer protection statute, the court may issue such orders or judgments as may be necessary to restore any person who has suffered any loss. If violation was willful, court may issue penalty up to three but not less than two times that amount. A person that experienced a breach of security shall not require a resident to waive the resident's private right of action as a condition of the offer of credit monitoring services.
Safeguards	No provision
Other provisions	Bulletin B-2010-2 (February 1, 2010)

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	MICHIGAN (8/23)
Citation	M.C.L.A. 445.61 to 445.73
Person Covered	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; a person or agency that maintains a database that includes data that the person or agency does not own or license that discovers a breach of the security of the database.
Notification of Breach (Required)	A covered person that owns or licenses data included in a database must notify affected residents of any breach if such breach is likely to cause substantial loss or injury or result in identity theft. A covered person that maintains a database must notify the owner or licensor of any breach if the breach is likely to cause substantial loss or injury or result in identity theft. Notice must be provided without unreasonable delay. If the covered person must notify more than 1,000 residents, notice must be given to all consumer reporting agencies that maintain files on consumers on a nationwide basis.
Notification of Breach (Delay/Exemption)	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. A law enforcement agency determines and advises the agency or person that providing a notice will impede a criminal or civil investigation or jeopardize homeland or national security.
Personal Information Defined (Encrypted/Unencrypted)	"Personal information" means the first name or first initial and last name linked to at least one other identifying element or in combination with sufficient information to identify and access the account, automated or electronic signature, biometrics, stock or other certificate or account number, credit card number, vital record, or medical records or information.
Breach of Security Defined	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. Good faith exception.
Penalties	Civil penalty for failure to provide notice of not more than $250 for each violation, but not more than $750,000 in the aggregate for violations that arise from the same security breach. Criminal penalty for notice of a security breach that has not occurred, with the intent to defraud, is a misdemeanor punishable to not more than 93 days imprisonment or a fine of $250 (or both) for each violation. These provisions do not affect the availability of any civil remedy for a violation of state or federal law.

MICHIGAN (cont.)

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	MICHIGAN (cont.)
Private Cause of Action/Enforcement	Yes. A person bringing an action under M.C.L.A. 445.67a(1) may recover actual damages including reasonable attorney fees or the lesser of either $5,000 per violation or $250,000 for each day that a violation occurs. The attorney general may also bring a civil action.
Safeguards	A person or agency that maintains a database that includes personal information regarding multiple individuals shall destroy any data that contains personal information concerning an individual when that data is removed from the database and the person or agency is not retaining the data elsewhere for another purpose not prohibited by state or federal law.
Other provisions	

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	MINNESOTA (8/23)
Citation	§§ 325E.61; 8.31
Person Covered	Any person or business that conducts business in this state, and that owns or licenses data that includes personal information and any person or business that maintains data that includes personal information that the person or business does not own.
Notification of Breach (Required)	A covered person that owns or licenses data that includes personal information shall notify any affected resident of any breach if personal information is reasonably believed to have been acquired by an unauthorized person. Notification must be made in the most expedient time possible and without unreasonable delay. A covered person that maintains data that includes personal information shall notify the owner or licensee of any breach immediately following discovery if the personal information is reasonably believed to have been acquired by an unauthorized person. If a covered person must provide notice to more than 500 residents, notice shall be given to all consumer reporting agencies that maintain files on consumers on a nationwide basis within 48 hours.
Notification of Breach (Delay/Exemption)	Notification may be delayed if law enforcement determines notification will impede a criminal investigation.
Personal Information Defined (Encryption/Unencrypted)	"Personal information" means an individual's first name or initial and last name in combination with any one or more other identifying 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. "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.
Breach of Security Defined	The unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith exception.
Penalties	No provision
Private Cause of Action/Enforcement	No, enforcement by attorney general only under M.S.A. § 8.31.
Safeguards	No provision
Other provisions	Any waiver of the provisions of this section is contrary to public policy and is void and unenforceable.

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	MISSISSIPPI (8/23)
Citation	§ 75-24-29
Person Covered	This section applies to any person who conducts business in this state and who, in the ordinary course of the person's business functions, owns, licenses or maintains personal information of any resident of this state. Any person who conducts business in this state that maintains computerized data which includes personal information that the person does not own or license.
Notification of Breach (Required)	A person who conducts business in this state shall disclose any breach of security to all affected individuals. The disclosure shall be made without unreasonable delay. Any person who maintains computerized data which includes personal information shall notify the owner or licensee of such information as soon as practicable.
Notification of Breach (Delay/Exemption)	Notification may be delayed if law enforcement determines notification will impede a criminal investigation or national security. Any such delayed notification shall be made after the law enforcement agency determines that notification will not compromise the criminal investigation or national security and so notifies the person of that determination.
Personal Information Defined (Encryption/Unencrypted)	"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. "Personal information" means an individual's first name or initial and last name in combination with any one or more other identifiable data elements and must not have been secured by encryption or any other method or technology that renders the personal information unreadable or unusable.
Breach of Security Defined	The unauthorized acquisition of electronic files, media, databases or computerized data containing personal information of any resident of the state when access is not encrypted. *See* general definitions.
Penalties	Violation of this section shall constitute an unfair trade practice.
Private Cause of Action/Enforcement	No, enforcement by attorney general only. Nothing in this section may be construed to create a private right of action.
Safeguards	No provision
Other provisions	

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	MISSOURI (8/23)
Citation	Mo. Rev. Stat. § 407.1500
Person Covered	Any person that owns or licenses personal information of residents of Missouri or any person that conducts business in Missouri that owns or licenses personal information in any form of a resident of Missouri. Any person that maintains or possesses records or data containing personal information of residents of Missouri that the person does not own or license, or any person that conducts business in Missouri that maintains or possesses records or data containing personal information of a resident of Missouri that the person does not own or license.
Notification of Breach (Required)	Any covered person shall notify the owner or licensee of the information of any breach of security immediately following discovery of the breach. Any covered person shall notify the affected persons of a breach. Notification shall be made without unreasonable delay. If an entity is required to notify more than 1,000 persons, the entity shall also notify the attorney general and all consumer reporting agencies that maintain files on consumers on a nationwide basis.
Notification of Breach (Delay/Exemption)	Notification may be delayed if law enforcement determines notification will impede a criminal investigation or jeopardize national or homeland security.
Personal Information Defined (Encryption/Unencrypted)	Personal information includes an individual's first name or initial and last name in combination with any one of another identifying elements and not encrypted, redacted, or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable or unusable. Personal information also includes 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.
Breach of Security Defined	The unauthorized access to and unauthorized acquisition of personal information maintained in a computerized form by a person that compromises the security, confidentiality, or integrity of the personal information. Good faith exception.
Penalties	Attorney general has exclusive authority to bring an action to obtain actual damages for a willful and knowing violation of this section and may seek a civil penalty not to exceed $150,000 per breach of the security system or series of breaches of a similar nature that are discovered in a single investigation.
Private Cause of Action/Enforcement	No, enforcement by attorney general only.
Safeguards	No provision
Other provisions	

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	MONTANA (8/23)
Citation	§§ 30-14-1701 to 30-14-1705
Person Covered	Any person or business that conducts business in Montana and that owns or licenses computerized data that includes personal information and any person or business that maintains computerized data that includes personal information that the person or business does not own.
Notification of Breach (Required)	Any covered person shall notify any resident whose personal information was or is reasonably believed to have been acquired by an unauthorized person. Disclosure must be made without unreasonable delay. Any person that is required to issue a notification pursuant to this section shall simultaneously submit an electronic copy of the notification and a statement providing the date and method of distribution to the attorney general's consumer protection office.
Notification of Breach (Delay/Exemption)	Notification may be delayed if law enforcement determines notification will impede a criminal investigation.
Personal Information Defined (Encrypted/Unencrypted)	"Personal information" means an individual's name, signature, address, or telephone number, in combination with one or more additional pieces of identifying information about the individual and the information in any form on an individual that is not encrypted. "Personal information" also includes: 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 that is lawfully made available to the general public from federal, state, or local government records.
Breach of Security Defined	The unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the person or business and causes or is reasonably believed to cause loss or injury to a Montana resident. Good faith exception.
Penalties	Penalties provided in § 30-14-142.
Private Cause of Action/Enforcement	No. Whenever the department has reason to believe that a person has violated this part and that proceeding would be in the public interest, the department may bring an action in the name of the state against the person to restrain by temporary or permanent injunction or temporary restraining order the use of the unlawful method, act, or practice upon giving appropriate notice to the person.
Safeguards	A business shall take all reasonable steps to destroy or arrange for the destruction of a customer's records containing personal information that is no longer necessary to be retained by modifying those records to make it unreadable or undecipherable.
Other provisions	

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	NEBRASKA (8/23)
Citation	§§ 87-801 to 87-808
Person Covered	An individual or a commercial entity that conducts business in Nebraska and that owns or licenses computerized data that includes personal information about a resident of Nebraska and an individual or a commercial entity that maintains computerized data that includes personal information that the individual or commercial entity does not own or license.
Notification of Breach (Required)	A business entity that owns or licenses computerized data that includes personal information shall notify affected state residents if an investigation determines that personal information has been or will be used for an unauthorized purpose. Any individual or commercial entity that maintains computerized data that includes personal information that it does not own or license shall give notice to the owner or licensee of a breach of security. The notice shall be made as soon as possible and without unreasonable delay. The individual or commercial entity shall also, not later than the time when the notice is provided to the Nebraska resident, provide notice of the breach to the attorney general.
Notification of Breach (Delay/Exemption)	Notification may be delayed if law enforcement determines notification will impede a criminal investigation.
Personal Information Defined (Encryption/Unencrypted)	"Personal information" means a resident's first name or first initial and last name in combination with another identifying data element that is not encrypted, redacted, or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable or unusable. Data shall not be considered encrypted if the confidential process or key was or is reasonably believed to have been acquired as a result of the breach of the security system. "Personal information" also includes: 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.
Breach of Security Defined	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 exception.
Penalties	Attorney general may issue subpoenas and seek and recover direct economic damages for each affected Nebraska resident injured by a violation of the act.
Private Cause of Action/Enforcement	No, enforcement by attorney general only. A violation does not give rise to a private cause of action.
Safeguards	An individual or a commercial entity that conducts business in Nebraska and owns, licenses, or maintains computerized data that includes personal information about a resident of Nebraska shall implement and maintain reasonable security procedures and practices that are appropriate to the nature and sensitivity of the personal information owned, licensed, or maintained and the nature and size of, and the resources available to, the business and its operations.
Other provisions	Any waiver of the provisions of the Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006 is contrary to public policy and is void and unenforceable.

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	NEVADA (8/23)
Citation	Nev. Rev. Stat. 603A.010 to 603A.920
Person Covered	Any data collector that owns or licenses computerized data which includes personal information and any data collector that maintains computerized data which includes personal information that the data collector does not own. "Data collector" means any governmental agency, institution of higher education, corporation, financial institution or retail operator or any other type of business entity or association that, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates, or otherwise deals with nonpublic personal information.
Notification of Breach (Required)	Any data collector that owns or licenses computerized data that includes personal information shall disclose a breach to any resident whose unencrypted information was or is reasonably believed to have been acquired by an unauthorized person. Any data collector who does not own the information shall notify the owner or licensee. Disclosure must be made in most expedient time possible and without unreasonable delay. Any covered person must also notify any consumer reporting agency that maintains files on consumers on a nationwide basis if a breach affects 1,000 or more persons at any one time.
Notification of Breach (Delay/Exemption)	Notification may be delayed if law enforcement determines notification will impede a criminal investigation.
Personal Information Defined (Encryption/Unencrypted)	"Personal information" means first name or first initial and last name in combination with another identifying data element in any form on an individual that is not encrypted. "Personal information" also includes: a medical identification number or a health insurance identification number; 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. "Personal information" does not include the last four digits of a social security number, the last four digits of a driver's license number, the last four digits of a driver authorization card number, or the last four digits of an identification card number or publicly available information that is lawfully made available to the general public from federal, state or local governmental records.
Breach of Security Defined	The unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information maintained by the data collector. Good faith exception.
Penalties	Attorney general may bring an action against any person violating this chapter to obtain a temporary or permanent injunction against the violation. The attorney general may also impose a civil penalty not to exceed $5,000 for each violation.

NEVADA (cont.)

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	NEVADA (cont.)
Private Cause of Action/Enforcement	It depends. The provisions of NRS 603A.300 to 603A.360 do not establish a private right of action against an operator. However, a data collector that provides notification may commence an action for damages against a person that unlawfully obtained or benefitted from personal information obtained from records maintained by the data collector.
Safeguards	A data collector that maintains records which contain personal information shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure. A contract for the disclosure of the personal information of a resident of Nevada which is maintained by a data collector must include a provision requiring the person to whom the information is disclosed to implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure.
Other provisions	"Covered information" means first name and last name or one or more elements of personally identifiable information about a consumer collected by an operator through an Internet website or online service and maintained by the operator or a data broker in an accessible form. Any waiver of the provisions of NRS 603A.010 to 603A.920, inclusive, is contrary to public policy, void and unenforceable.

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	NEW HAMPSHIRE (8/23)
Citation	N.H. Rev. Stat. §§ 359-C:19 to 359-C:21
Person Covered	Any person doing business in this state who owns or licenses computerized data that includes personal information and any person or business that maintains computerized data that includes personal information that the person or business does not own.
Notification of Breach (Required)	Any person who owns or licenses computerized data shall determine if after a breach the likelihood that the information has been or will be misused and shall notify the affected persons. Any person engaged in trade or commerce shall also notify the regulator which has primary regulatory authority over such trade or commerce. All other persons shall notify the state attorney general's office. Any covered person shall notify the affected individuals of a breach as soon as possible. Any person or business that maintains computerized data that includes personal information that they do not own shall notify the owner or licensee. If a person is required to notify more than 1,000 consumers of a breach of security pursuant to this section, the person shall also notify, without unreasonable delay, all consumer reporting agencies that maintain files on consumers on a nationwide basis.
Notification of Breach (Delay/Exemption)	Notification may be delayed if law enforcement determines notification will impede a criminal investigation or national or homeland security.
Personal Information Defined (Encrypted/Unencrypted)	"Personal information" means first name or first initial and last name in combination with another identifying element in any form on an individual when either the name or the data elements are not encrypted. "Personal Information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.
Breach of Security Defined	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 exception.
Penalties	Injured person may bring an action for damages and for such equitable relief, including an injunction, as the court deems necessary and proper. If the court finds the action was a willful violation, it shall award as much as three times, but no less than two times, such amount. When action brought by attorney general, civil penalties up to $10,000 per violation. See RSA 358-A:4.
Private Cause of Action/Enforcement	Yes, attorney general or any injured person may bring an action.
Safeguards	No provision
Other provisions	Any attempted waiver of the right to the damages shall be void and unenforceable.

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	NEW JERSEY (8/23)
Citation	N.J.S.A. 56:8-161 to 56:8-166.1
Person Covered	Any business that conducts business in New Jersey, or any public entity that compiles or maintains computerized records that include personal information and any business or public entity that compiles or maintains computerized records that include personal information on behalf of another business or public entity.
Notification of Breach (Required)	Any covered person shall disclose any breach of security to any customer who is a resident of New Jersey whose information was or, is reasonably believed to have been accessed by unauthorized persons. Notification shall be made in the most expedient time possible and without unreasonable delay. Any covered person required to disclose a breach of security shall report the breach to the division of state police. Any business or public entity that compiles or maintains computerized records that include personal information on behalf of another business or public entity shall notify that business or public entity of any security breach. When a business or public entity discovers circumstances requiring notification pursuant to this section of more than 1,000 persons at one time, the business or public entity shall also notify, without unreasonable delay, all consumer reporting agencies that maintain files on consumers on a nationwide basis.
Notification of Breach (Delay/Exemption)	Notification may be delayed if law enforcement determines notification will impede a criminal investigation.
Personal Information Defined (Encryption/Unencrypted)	"Personal information" means an individual's first name or first initial and last name in combination with another identifying element that is not secured by encryption or by any other method or technology that renders the personal information unreadable or unusable. 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.
Breach of Security Defined	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 exception.
Penalties	It shall be an unlawful practice and a violation of P.L. 1960, c. 39 (C. 56:8-1 et seq.) to willfully, knowingly or recklessly violate these sections.

NEW JERSEY (cont.)

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	NEW JERSEY (cont.)
Private Cause of Action/Enforcement	No
Safeguards	A business or public entity shall destroy, or arrange for the destruction of, a customer's records within its custody or control containing personal information, which is no longer to be retained by the business or public entity, by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable, undecipherable, or nonreconstructable through generally available means.
Other provisions	Bulletin 2007-10

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	NEW MEXICO (8/23)
Citation	N.M. Stat. Ann. §§ 57-12C-1 to 57-12C-12
Person Covered	Any person doing business in this state who owns or licenses computerized elements that includes personal information any person that maintains computerized data that includes personal information that the person does not own.
Notification of Breach (Required)	A person that owns or licenses elements that include personal identifying information of a New Mexico resident shall provide notification to each New Mexico resident whose personal identifying information is reasonably believed to have been subject to a security breach. Notification shall be made in the most expedient time possible, but not later than 45 calendar days following discovery of the security breach. Any person that is licensed to maintain or possess computerized data containing personal identifying information of a New Mexico resident that the person does not own or license shall notify the owner or licensee of the information of any security breach in the most expedient time possible, but not later than 45 calendar days following discovery of the breach. A person that is required to issue notification to more than 1,000 New Mexico residents as a result of a single security breach shall notify the office of the attorney general and major consumer reporting agencies that maintain files on consumers on a nationwide basis in the most expedient time possible, but no later than 45 calendar days.
Notification of Breach (Delay/Exemption)	Notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation; or as necessary to determine the scope of the security breach and restore the integrity, security and confidentiality of the data system.
Personal Information Defined (Encrypted/Unencrypted)	"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. 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.
Breach of Security Defined	The unauthorized acquisition of unencrypted computerized data, or of encrypted computerized data and the confidential process or key used to decrypt the encrypted computerized data, that compromises the security, confidentiality, or integrity of personal identifying information maintained by a person. Good faith exception.
Penalties	The court may issue an injunction and award damages for actual costs or losses. The court may impose a civil penalty of the greater of $25,000, or $10 per instance of failed notification up to a maximum of $150,000.

NEW MEXICO (cont.)

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	NEW MEXICO (cont.)
Private Cause of Action/Enforcement	The attorney general may bring an action on the behalf of individuals and in the name of the state.
Safeguards	A person that owns or licenses records containing personal identifying information of a New Mexico resident shall arrange for proper disposal of the records when they are no longer reasonably needed for business purposes. A person that owns or licenses personal identifying information of a New Mexico resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal identifying information from unauthorized access, destruction, use, modification or disclosure.
Other provisions	

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	NEW YORK (8/23)
Citation	Bus. § 899-aa; Tech. § 208
Person Covered	Any person or business which owns or licenses computerized data which includes private information and any person or business which maintains computerized data which includes private information which such person or business does not own.
Notification of Breach (Required)	Any entity that owns or licenses computerized data in the state shall disclose any breach to any New York residents whose private information was or is reasonably believed to have been acquired by unauthorized persons. Any entity which maintains computerized data which contains personal information shall notify the owner or licensee of any breach if the information was or is reasonably believed to have been acquired by unauthorized persons. The disclosure shall be made in the most expedient time possible and without unreasonable delay. In the event that more than 5,000 New York residents are to be notified of a breach, the entity shall also notify consumer reporting agencies.
Notification of Breach (Delay/Exemption)	Notification may be delayed if law enforcement determines notification will impede a criminal investigation.
Personal Information Defined (Encryption/Unencrypted)	"Private information" means the combination of name, number, personal mark, or other identifier in combination with a data element such as social security number, driver's license number, etc. The data element is not encrypted, or encrypted with an encryption key that has also been acquired. "Private information" does not include publicly available information which is lawfully made available to the general public from federal, state, or local government records.
Breach of Security Defined	Unauthorized access to or acquisition of, or access to or acquisition without valid authorization, of computerized data that compromises the security, confidentiality, or integrity of private information maintained by a business. Good faith exception.
Penalties	Injunctive relief. If the violation was knowing or reckless, the court may impose a civil penalty of the greater of $5,000 or up to $20 per instance of failed notification, provided that the latter amount shall not exceed $250,000.
Private Cause of Action/Enforcement	No, enforcement by attorney general only. Three-year statute of limitations.
Safeguards	No provision
Other provisions	General Counsel Opinion 12-2-2005

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	NORTH CAROLINA (8/23)
Citation	§§ 75-61; 75-64; 75-65
Person Covered	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). Any business that maintains or possesses records or data containing personal information of residents of North Carolina that the business does not own or license, or any business that conducts business in North Carolina that maintains or possesses records or data containing personal information that the business does not own or license.
Notification of Breach (Required)	Any entity that owns or licenses personal information shall notify the affected persons of a breach following discovery or notification of the breach. Any entity that maintains or possesses personal information that the entity does not own or license the personal information shall notify the owner or licensee of a breach. Notification shall be made without unreasonable delay. Any covered person shall notify the Consumer Protection Division of the Attorney General's Office and all consumer reporting agencies if the entity is to notify more than 1,000 persons.
Notification of Breach (Delay/Exemption)	Notification may be delayed if law enforcement informs the business that notification will impede a criminal investigation or jeopardize national or homeland security.
Personal Information Defined (Encryption/Unencrypted)	"Personal information" means a person's first name or first initial and last name in combination with another identifying element in any form on an individual that is not encrypted or redacted. "Personal information" does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed.
Breach of Security Defined	An incident of unauthorized access to and acquisition of unencrypted and unredacted records or data containing personal information where illegal use of the personal information has occurred or is reasonably likely to occur or that creates a material risk of harm to a consumer. Good faith exception.
Penalties	No provision
Private Cause of Action/Enforcement	Yes, but only if the individual is injured as a result of the violation. A violation of this statute is a violation of § 75-1.1.

NORTH CAROLINA (cont.)

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	NORTH CAROLINA (cont.)
Safeguards	Any business that conducts business in North Carolina and maintains or possesses personal information of a resident of North Carolina, must take reasonable measures, including destruction of personal information records, to protect against unauthorized access. This provision does not apply to banks, financial institutions, health insurers, health care facilities, and consumer reporting agencies who are in compliance with federal privacy legislation.
Other provisions	Any waiver of the provisions of this Article is contrary to public policy and is void and unenforceable. Causes of action arising under this Article may not be assigned.

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	NORTH DAKOTA (8/23)
Citation	§§ 51-30-01 to 51-30-07; 51-15-11
Person Covered	Any person that conducts business in this state, and that owns or licenses computerized data that includes personal information and any person that maintains computerized data that includes personal information that the person does not own.
Notification of Breach (Required)	Any person that conducts business that owns, or licenses computerized data shall disclose any breach of security immediately following the discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Any person that maintains computerized data that the person does not own shall notify the owner or licensee immediately following the breach. Any covered person must notify the attorney general if a breach affects more than 250 persons. Disclosures must be made in the most expedient time possible and without unreasonable delay.
Notification of Breach (Delay/Exemption)	Notification may be delayed if law enforcement determines notification will impede a criminal investigation.
Personal Information Defined (Encryption/Unencrypted)	"Personal information" means information in any form on an individual that is not encrypted. "Personal information" means an individual's first name or first initial and last name in combination with any one of the following data elements, when the name and data elements are not encrypted: 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.
Breach of Security Defined	The 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 exception.
Penalties	The court may assess for the benefit of the state a civil penalty of not more than $5,000 for each violation.
Private Cause of Action/Enforcement	No, enforcement by attorney general only.
Safeguards	No provision
Other provisions	

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	OHIO (8/23)
Citation	§§ 1347.12; 1349.19; 1349.191; 1349.192
Person Covered	Any state agency or agency of a political subdivision that owns or licenses computerized data that includes personal information and any state agency or agency of a political subdivision that, on behalf of or at the direction of another state agency or agency of a political subdivision, is the custodian of or stores computerized data that includes personal information. Any person that owns or licenses computerized data that includes personal information and any person that, on behalf of or at the direction of another person or on behalf of or at the direction of any governmental entity, is the custodian of or stores computerized data that includes personal information.
Notification of Breach (Required)	Any covered person shall disclose any breach of security following its discovery or notification to any resident of the state if the personal information was or is reasonably believed to have been acquired by unauthorized persons. Disclosure shall be made in the most expedient time possible but no later than 45 days following its discovery or notification of a breach. If a breach affects more than 1,000 residents, any covered person shall notify all consumer reporting agencies that maintain files on consumers on a nationwide basis.
Notification of Breach (Delay/Exemption)	Notification may be delayed if law enforcement determines notification will impede a criminal investigation or jeopardize homeland or national security.
Personal Information Defined (Encryption/Unencrypted)	"Personal information" means an individual's first name or first initial and last name in combination with another identifying element that is not encrypted, redacted, or altered by any method or technology in such a manner that the data elements are unreadable. "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 media that is widely distributed.
Breach of Security Defined	Unauthorized access to and acquisition of computerized data that compromises the security or confidentiality of personal information owned or licensed by a state agency or an agency of a political subdivision and that causes, reasonably is believed to have caused, or reasonably is believed will cause a material risk of identity theft or other fraud to the person or property of an Ohio resident. Good faith exception.

OHIO (cont.)

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	OHIO (cont.)
Penalties	Civil penalty of up to $1,000 for each day person, state agency, or agency of a political subdivision has intentionally or recklessly failed to comply for the first 60 days, up to $5,000 for each day of noncompliance beginning on the 61st day to the 90th day, and up to $10,000 for each day of noncompliance on the 91st day and after.
Private Cause of Action/Enforcement	No, enforcement by attorney general only.
Safeguards	No provision
Other provisions	Any waiver of this section is contrary to public policy and is void and unenforceable. This section does not apply to any person or entity that is a covered entity as defined by 45 C.F.R. § 160.103.

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	OKLAHOMA (8/23)
Citation	24 Okl.St.Ann. §§ 161 to 166; 74 Okl.St.Ann. § 3113.1
Person Covered	An individual or entity that owns or licenses computerized data that includes personal information and an individual or entity that maintains computerized data that includes personal information that the individual or entity does not own or license. Any state agency, board, commission or other unit or subdivision of state government that owns or licenses computerized data that includes personal information; any state agency, board, commission or other unit or subdivision of state government that maintains computerized data that includes personal information it does not own.
Notification of Breach (Required)	Any covered person shall notify any resident of the state whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed by unauthorized persons that causes or the entity reasonably believes has or will cause identity theft or fraud. Notice shall be made without unreasonable delay. Any person that maintains computerized data that the entity does not own shall notify the owner or licensee of the information after a breach without unreasonable delay.
Notification of Breach (Delay/Exemption)	Notification may be delayed if law enforcement determines notification will impede a criminal investigation or jeopardize homeland or national security.
Personal Information Defined (Encryption/Unencrypted)	"Personal information" means first name or first initial and last name in combination with another identifying data element in any form on an individual that is neither encrypted nor redacted. "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.
Breach of Security Defined	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 pr will cause, identity theft or other fraud to any resident of Oklahoma. Good faith exception.
Penalties	Civil penalty not to exceed $150,000 per breach of the security system or series of breaches of a similar nature that are discovered in a single investigation, or actual damages.
Private Cause of Action/Enforcement	No, enforcement by attorney general or district attorney. A violation by a state-chartered or state-licensed institution shall be enforceable exclusively by the primary state regulator of the financial institution.
Safeguards	No provision
Other provisions	

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	OREGON (8/23)
Citation	Or. Rev. Stat. §§ 646A.600; 646A.602; 646A.604; 646A.622; 646A.624; 646A.626
Person Covered	An individual or entity that owns, licenses, maintains, stores, manages, collects, processes, acquires or otherwise possesses personal information in the course of the person's business, vocation, occupation or volunteer activities. Does not include a person who acts solely as a vendor.
Notification of Breach (Required)	A person that conducts business in the state and that owns, or licenses personal information shall give notice of a breach to the affected consumer. Any person that maintains or possess personal information shall notify the owner or licensee. If a covered entity is subject to a breach of security or receives notice of a breach of security from a vendor, the covered entity shall give notice to the Attorney General if more than 250 consumers are affected. The notification must be made in the most expeditious manner possible and without unreasonable delay, but not later than 45 days after discovering the breach. Any covered person shall notify all consumer reporting agencies if the breach affects more than 1,000 consumers. The notification shall be without unreasonable delay and shall include any police report number assigned to the breach.
Notification of Breach (Delay/Exemption)	Notification may be delayed if law enforcement determines notification will impede a criminal investigation. A person does not need to notify consumers of a breach of security if, after an appropriate investigation or after consultation with relevant federal, state or local law enforcement agencies, the person reasonably determines that the consumers whose personal information was subject to the breach of security are unlikely to suffer harm. The person must document the determination in writing and maintain the documentation for at least 5 years.
Personal Information Defined (Encryption/Unencrypted)	"Personal information" means an individual's first name or first initial and last name in combination with another identifying data element in any form on an individual that is not encrypted or redacted, or is encrypted and the encryption key has been accessed or acquired. "Personal information" also includes: identification number issued by a foreign nation; passport number or other United States-issued identification number; 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; or any information about a consumer's medical history or mental or physical condition or about a health care professional's medical diagnosis or treatment of the consumer. "Personal information" does not include publicly available information, other than a social security number, that is lawfully made available to the general public from federal, state or local government records.

OREGON (cont.)

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	OREGON (cont.)
Breach of Security Defined	An 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.
Penalties	A violation of this chapter is an unlawful practice under ORS 646.607. Any person who violates this section shall be subject to a penalty of not more than $1,000 for every violation, which shall be paid to the general fund of the state treasury. Every violation is a separate offense, and, in the case of a continuing violation, each day’s continuance is a separate violation. Maximum penalty shall not exceed $500,000.
Private Cause of Action/Enforcement	No, enforcement by the director of the department of consumer and business services.
Safeguards	A person that owns, maintains, or otherwise possesses, or has control over or access to, shall develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the personal information, including safeguards that protect the personal information when the person disposes of the personal information.
Other provisions	

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	PENNSYLVANIA (8/23)
Citation	73 Pa. Stat. Ann. §§ 2302 to 2308
Person Covered	An entity that maintains, stores or manages computerized data that includes personal information and a vendor that maintains, stores or manages computerized data on behalf of another entity.
Notification of Breach (Required)	Any covered person shall provide notice of any breach to any resident of the state whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed by unauthorized persons. Notice shall be made without unreasonable delay. When an entity provides notification under this act to more than 1,000 persons at one time, the entity shall also notify, without unreasonable delay, all consumer reporting agencies that maintain files on consumers on a nationwide basis.
Notification of Breach (Delay/Exemption)	Notification may be delayed if law enforcement determines notification will impede a criminal or civil investigation.
Personal Information Defined (Encrypted/Unencrypted)	"Personal information" means an individual's first name or first initial and last name in combination with another identifying data element in any form on an individual that is not encrypted or redacted. "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.
Breach of Security Defined	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 exception.
Penalties	Violation of this act shall be deemed to be an unfair deceptive act or practice in violation of the Unfair Trade Practices and Consumer Protection Law.
Private Cause of Action/Enforcement	No, enforcement by attorney general only.
Safeguards	An entity that maintains, stores or manages computerized data on behalf of Pennsylvania that constitutes personal information shall utilize encryption, or other appropriate security measures, to reasonably protect the transmission of personal information over the Internet from being viewed or modified by an unauthorized third party. The aforementioned entity shall also develop a policy to govern reasonably proper storages of the personal information.
Other provisions	This act shall supersede and preempt all rules, regulations, codes, statutes or ordinances of all cities, counties, municipalities, and other local agencies within the Commonwealth.

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	PUERTO RICO (8/23)
Citation	10 L.P.R.A. §§ 4051 to 4055
Person Covered	Any entity that is the owner or custodian of a database that includes personal information of citizens residents of Puerto Rico and any entity that as part of their operations resells or provides access to digital data banks that at the same time contain personal information files of citizens.
Notification of Breach (Required)	Any covered person shall notify affected persons of any breach when the personal information is unencrypted. Notification must be as expeditious as possible. Any covered person must notify the department within 10 days which shall then make a public announcement within 24 hours of receiving the information.
Notification of Breach (Delay/Exemption)	No provision
Personal Information Defined (Encrypted/Unencrypted)	"Personal information file" means a file containing at least the name or first initial and surname of a person in combination with another identifying element and is legible enough to be accessed without the use of a special cryptographic code. "Personal information" also includes medical information protected by HIPAA; tax information; work-related evaluations. "Personal information" does not include the mailing or the residential address or information that is a public document and that is available to the citizens in general.
Breach of Security Defined	"Violation of the security system" means any situation in which it is detected that access has been permitted to unauthorized persons or entities to the data files so that the security, confidentiality or integrity of the information in the data bank has been compromised; or when normally authorized persons or entities have had access and it is known or there is reasonable suspicion that they have violated the professional confidentiality or obtained authorization under false representation with the intention of making illegal use of the information.
Penalties	The secretary may impose fines of $500 up to $5,000 for each violation of this chapter.
Private Cause of Action/Enforcement	The fines provided do not affect the rights of the consumers to initiate actions or claims for damages.
Safeguards	No provision
Other provisions	

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	RHODE ISLAND (8/23)
Citation	§§ 11-49.3-1 to 11-49.3-6
Person Covered	Any state agency or person that owns, maintains or licenses computerized data that includes personal information and any state agency or person that maintains computerized unencrypted data that includes personal information that the state agency or person does not own.
Notification of Breach (Required)	Any covered person shall provide notification of a breach which poses a risk of identity theft whose personal information was or is reasonably believed to have been accessed by unauthorized persons to the affected person. The notification shall be made in the most expedient time possible but no later than 45 days after confirmation of the breach. If more than 500 Rhode Island residents are to be notified, any covered person shall notify the attorney general and the major credit reporting agencies. Notification shall be made without delay.
Notification of Breach (Delay/Exemption)	Notification may be delayed if law enforcement determines notification will impede a criminal investigation.
Personal Information Defined (Encryption/Unencrypted)	"Personal information" means an individual's first name or first initial and last name in combination with any one or more identifying elements in any form on an individual that is not encrypted or is in hard copy. "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.
Breach of Security Defined	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 exception.
Penalties	Each reckless violation is subject to a penalty of not more than $100 per record. Each knowing and willful violation is subject to a penalty of not more than $200 per record.
Private Cause of Action/Enforcement	No, enforcement by attorney general only.
Safeguards	A municipal agency, state agency or person that stores, collects, processes, maintains, acquires, uses, owns or licenses personal information about a Rhode Island resident shall implement and maintain a risk-based information security program which contains reasonable security procedures and practices appropriate to the size and scope of the organization, the nature of the information and the purpose for which the information was collected.
Other provisions	

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	SOUTH CAROLINA (8/23)
Citation	S.C. Code § 39-1-90
Person Covered	A person conducting business in this state and owning or licensing computerized data or other data that includes personal identifying information and a person conducting business in this state and maintaining computerized data or other data that includes personal identifying information that the person does not own.
Notification of Breach (Required)	Any covered person shall disclose a breach immediately following discovery to a resident of the state whose personal information that was unencrypted or unredacted 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. If a business is required to notify more than 1,000 residents at one time, the business shall also notify, without unreasonable delay, the Consumer Protection Division of the Department of Consumer Affairs and all consumer reporting agencies.
Notification of Breach (Delay/Exemption)	Notification may be delayed if law enforcement determines notification will impede a criminal investigation.
Personal Information Defined (Encryption/Unencrypted)	"Personal information" means the first name or first initial and last name in combination with another identifying data element in any form on an individual that is neither encrypted nor redacted. "Personal identifying information" does not include information that is lawfully obtained from publicly available information, or from federal, state, or local governmental records lawfully made available to the general public.
Breach of Security Defined	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 exception.
Penalties	Knowing and willful violation is subject to an administrative fine in the amount of $1,000 for each resident whose information was accessible by reason of the breach.
Private Cause of Action/Enforcement	Yes, a resident of this state who is injured by a violation of this section may institute a civil action to recover damages in the case of a knowing and willful violation, institute a civil action that must be limited to actual damages resulting from a negligent violation, seek an injunction to enforce compliance, and, if successful, recover attorney's fees and court costs.
Safeguards	No provision
Other provisions	

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	SOUTH DAKOTA (8/23)
Citation	SDCL §§ 22-40-19 to 22-40-26
Person Covered	"Information holder" means any person or business that conducts business in this state, and that owns or licenses computerized personal or protected information of residents of this state.
Notification of Breach (Required)	Following the discovery by or notification to an information holder of a breach of system security an information holder shall disclose the breach of system security to any resident of this state whose personal or protected information was or is reasonably believed to have been, acquired by an unauthorized person. A disclosure under this section shall be made not later than 60 days from the discovery or notification of the breach of system security. An information holder shall also notify, without reasonable delay, all consumer agencies and any credit bureau or agency that maintains files on summers on a nationwide basis. Any information holder that experiences a breach of system security shall disclose to the attorney general any breach of system security that exceeds 250 residents of this state.
Notification of Breach (Delay/Exemption)	Notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. In the event of a delay, the notification shall be made no later than 30 days after law enforcement determines that notification will not compromise the investigation.
Personal Information Defined (Encryption/Unencrypted)	"Personal information" means a person's first name or first initial and last name, in combination with any one or more data elements. The term does not include information that is lawfully made available to the general public from federal, state, or local government records or information that has been redacted, or otherwise made unusable.
Breach of Security Defined	The unauthorized acquisition of unencrypted computerized data or encrypted computerized data and the encryption key by any person that materially compromises the security, confidentiality, or integrity of personal or protected information maintained by the information holder. Good faith exception.
Penalties	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 under this section.
Private Cause of Action/Enforcement	The attorney general may prosecute each failure to disclose under the provisions of this act as a deceptive act or practice under § 37-24-6.
Safeguards	No provision
Other provisions	

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	TENNESSEE (8/23)
Citation	Tenn. Code §§ 47-18-2104 to 47-18-2107
Person Covered	Any person or business that conducts business in this state, or any agency of the state of Tennessee or any of its political subdivisions, that owns or licenses computerized data that includes personal information. "Information holder" means any person or business that conducts business in this state, or any agency of this state or any of its political subdivisions, that owns, or licenses computerized personal information of residents of this state.
Notification of Breach (Required)	Any covered person shall disclose any breach of security to any resident of the state whose unencrypted personal information was or is reasonably believed to have been acquired by unauthorized persons. Any information holder that maintains computerized data that the holder does not own shall notify the owner or licensee. The disclosure shall be made in the most expedient time possible and without unreasonable delay, but no later than 45 days from the discovery. If notification is required to be given to more than 1,000 persons, the entity also shall report the breach, without unreasonable delay, to all consumer reporting agencies and credit bureaus.
Notification of Breach (Delay/Exemption)	Notification may be delayed if law enforcement determines notification will impede a criminal investigation.
Personal Information Defined (Encryption/Unencrypted)	“Personal information” means an individual’s first name or first initial and last name in combination with another identifying element in any form on an individual. “Personal information” does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.
Breach of Security Defined	The acquisition of unencrypted computerized data or encrypted computerized data and the encryption key by an unauthorized person that materially compromises the security, confidentiality, or integrity of personal information maintained by the information holder. Good faith exception.
Penalties	Any violation of this part constitutes a violation of the Tennessee Consumer Protection Act. A violation of this part shall be punishable by a civil penalty of whichever of the following is greater: $10,000; $5,000 per day for each day that a person's identity has been assumed; or 10 times the amount obtained or attempted to be obtained by the person using the identity theft.
Private Cause of Action/Enforcement	Yes, any customer who is a person or business entity injured by a violation may institute a civil action to recover damages as well as injunctive relief.
Safeguards	No provision
Other provisions	

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	TEXAS (8/23)
Citation	Tex. Bus. & Com. Code §§ 521.001 to 521.152
Person Covered	A person who conducts business in this state and owns or licenses computerized data that includes sensitive personal information and any person who maintains computerized data that includes sensitive personal information not owned by the person.
Notification of Breach (Required)	Any covered person shall disclose any breach of security to any individual whose information was or is reasonably believed to have been acquired by unauthorized persons not later than the 60th day after the date on which the person determines that the breach occurred. In cases involving at least 250 residents, the attorney general shall be notified as soon as practicable, and no later than the 30th day after the date on which the person determined the breach occurred, and must be submitted electronically using a form accessed through the attorney general's Internet website. Any entity that maintains computerized data that the entity does not own shall notify the owner or licensee immediately after discovering the breach if the information was or is reasonably believed to have been acquired by an unauthorized person. If notification is to be made to more than 10,000 persons, notification must also be made to each consumer reporting agency that maintains files on consumers on a nationwide basis. Notification shall be made without unreasonable delay.
Notification of Breach (Delay/Exemption)	Notification may be delayed if law enforcement determines notification will impede a criminal investigation.
Personal Information Defined (Encryption/Unencrypted)	"Personal information" means information that alone or in conjunction with other information identifies an individual. "Sensitive personal information" means an individual's first name or first initial and last name in combination with any one or more data items, if the name and the items are not encrypted. It does not include publicly available information that is lawfully made available to the public from the federal government or a state or local government. "Personal information" also includes 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, telecommunication access device, the physical or mental health or condition of the individual, the provision of health care to the individual, or payment for the provision of health care to the individual.
Breach of Security Defined	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 exception.

TEXAS (cont.)

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	TEXAS (cont.)
Penalties	A person who violates this chapter is liable for a civil penalty of at least $2,000 but not more than $50,000 for each violation. In addition, a person who fails to provide notice under this chapter is liable for a civil penalty of not more than $100 for each individual to whom notification is due for each consecutive day that the person fails to provide notification. Civil penalties under this section may not exceed $250,000 for all individuals to whom notification is due after a single breach.
Private Cause of Action/Enforcement	No, enforcement by attorney general only.
Safeguards	A business shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect from unlawful use or disclosure any sensitive personal information collected or maintained by the business in the regular course of business.
Other provisions	

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	UTAH (8/23)
Citation	Utah Code §§ 13-44-102 to 13-44-301
Person Covered	A person who owns or licenses computerized data that includes personal information concerning a Utah resident and a person who maintains computerized data that includes personal information that the person does not own or license.
Notification of Breach (Required)	Any covered person shall notify any affected resident when personal information was or is reasonably believed to have been accessed and acquired for identity theft or fraud purposes. Any person who owns or maintains computerized data that contains personal information shall notify the owner or licensee. Notification shall be made in the most expedient time possible without unreasonable delay. If an investigation reveals the misuse of personal information relating to 500 or more Utah residents, for identity theft or fraud purposes, the person shall also provide notification to the Office of Attorney General and the Utah Cyber Center. In the case of 1,000 Utah residents, the person shall provide notification to the Office of the Attorney General, Utah Cyber Center, and each national consumer reporting agency.
Notification of Breach (Delay/Exemption)	Notification may be delayed if law enforcement determines notification will impede a criminal investigation.
Personal Information Defined (Encryption/Unencrypted)	"Personal information" means a person's first name or first initial and last name when combined with another identifying data element and the name or date element is not encrypted or not protected by another method that renders the data unreadable or unusable. "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.
Breach of Security Defined	An unauthorized acquisition of computerized data maintained by a person that compromises the security, confidentiality, or integrity of personal information. "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.
Penalties	A person who violates this chapter is subject to a civil fine of not more than $2,500 for a violation or series of violations concerning a specific consumer, and no greater than $100,000 in the aggregate for related violations concerning more than one consumer, unless the violations concern 10,000 or more residents or non-residents or the person agrees to settle for a greater amount. The attorney general may also seek injunctive relief and attorney fees and costs.
Private Cause of Action/Enforcement	No, enforcement by attorney general only.
Safeguards	Any person who conducts business in the state and maintains personal information shall implement and maintain reasonable procedures to prevent unlawful use or disclosure of personal information maintained or collected in the regular course of business.
Other provisions	A waiver of disclosure is contrary to public policy and is void and unenforceable.

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	VERMONT (8/23)
Citation	9 V.S.A. §§ 2430 to 2435
Person Covered	Any data collector that owns or licenses computerized personally identifiable information that includes personal information concerning a consumer. Any data collector that maintains or possesses computerized data containing personally identifiable information of a consumer that the data collector does not own or license or any data collector that acts or conducts business in Vermont that maintains or possesses records or data containing personally identifiable information that the data collector does not own or license. "Data collector" means a person who, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates, or otherwise deals with personally identifiable information, and includes state, state agencies, political subdivisions of the state, public and private universities, privately and publicly held corporations, limited liability companies, financial institutions, and retail operators.
Notification of Breach (Required)	Any covered person shall notify the affected consumer following discovery or notification of the breach. Notice of the breach should be made in the most expedient time possible and without unreasonable delay, but no later than 45 days. Any data collector that maintains or possess computerized data that the entity does not own shall notify the owner or licensee. Any covered person shall provide notice to the department or the attorney general within 14 days of discovery or notification of the breach. Any covered person shall notify, without unreasonable delay, all consumer reporting agencies that maintain files on consumers on a nationwide basis if the entity must notify more than 1,000 persons at one time.
Notification of Breach (Delay/Exemption)	Notification may be delayed if law enforcement determines notification will impede a criminal investigation or jeopardize homeland or national security.
Personal Information Defined (Encryption/Unencrypted)	“Personally identifiable information” means a consumer’s first name or first initial and last name in combination with another identifying data element and the name, or the data elements are not encrypted or redacted or protected by another method that renders them unreadable or unusable. “Personally identifiable information” includes login credentials. “Personally identifiable information” does not mean publicly available information that is lawfully made available to the general public from federal, state, or local government records.

VERMONT (cont.)

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	VERMONT (cont.)
Breach of Security Defined	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. Good faith exception.
Penalties	Penalties may be assessed as provided under Chapter 63, Consumer Protection.
Private Cause of Action/Enforcement	No, enforcement by attorney general and state's attorney only.
Safeguards	No provision
Other provisions	

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	VIRGIN ISLANDS (8/23)
Citation	V.I. Code tit. 14, §§ 2206 to 2212
Person Covered	Any agency that owns or licenses computerized data that includes personal information and any agency that maintains computerized data that includes personal information that the agency does not own.
Notification of Breach (Required)	Any person that owns or licenses computerized data shall disclose any breach to any affected resident whose unencrypted personal information was or is reasonably believed to have been acquired by unauthorized persons. Any agency that maintains computerized data that the agency does not own shall notify the owner or licensee. Disclosure must be made in most expedient time possible and without unreasonable delay.
Notification of Breach (Delay/Exemption)	Notification may be delayed if law enforcement determines notification will impede a criminal investigation.
Personal Information Defined (Encryption/Unencrypted)	"Personal information" means an individual's first name or first initial and last name in combination with another identifying data element when either the name or the data elements are not encrypted. "Personal information" means information in any form on an individual that is not encrypted. "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or territorial government records.
Breach of Security Defined	Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith exception.
Penalties	Any business that violates or proposes to violate this title may be enjoined.
Private Cause of Action/Enforcement	Yes, any customer injured by a violation of this title may commence a civil action to recover damages.
Safeguards	No provision
Other provisions	Any waiver of notification is contrary to public policy, and is void and unenforceable.

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	VIRGINIA (8/23)
Citation	Va. Code §§ 18.2-186.6; 32.1-127.1:05; 59.1-575 to 59.1-584
Person Covered	An individual or entity that owns or licenses computerized data that includes personal information and an individual or entity that maintains computerized data that includes personal information that the individual or entity does not own or license.
Notification of Breach (Required)	Any covered individual shall notify any affected individual, owner, or licensee of the computerized data if the unencrypted or unredacted personal information was or is reasonably believed to have been accessed by unauthorized persons or if the information was or is reasonably likely to be used for identity theft or fraud. Notice shall be made without unreasonable delay. Any covered person shall notify the attorney general and all consumer reporting agencies that files on consumers on a nationwide basis if the entity is required to provide notification to more than 1,000 persons at one time. If unencrypted or unredacted medical information was or is reasonably believed to have been accessed and acquired by an unauthorized person, an entity that owns or licenses computerized data that includes medical information shall disclose any breach to the office of the attorney general, the commissioner of health, the subject of the medical information, and any affected resident of the Commonwealth without unreasonable delay.
Notification of Breach (Delay/Exemption)	Notification may be delayed if law enforcement determines notification will impede a criminal investigation or jeopardize homeland or national security.
Personal Information Defined (Encryption/Unencrypted)	"Personal information" the first name or first initial and last name in combination with another identifying element in any form on an individual that is neither encrypted nor redacted. It also includes medical information. "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. "Personal data" means any information that is linked or reasonably linkable to an identified or identifiable natural person.
Breach of Security Defined	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 exception.

VIRGINIA (cont.)

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	VIRGINIA (cont.)
Penalties	Attorney General may bring an action to impose a civil penalty not more than $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 shall limit an individual from recovering direct economic damages from a violation of this section. Attorney General may seek an injunction or up to $7,500 for each violation of the Consumer Data Protection Act.
Private Cause of Action/Enforcement	Yes, enforcement by attorney general or individuals. A violation by a state-chartered or licensed financial institution shall be enforceable exclusively by the financial institution's primary state regulator. A violation by an individual or entity regulated by the state corporation commission's bureau of insurance shall be enforced exclusively by the state corporation commission.
Safeguards	A data controller shall establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data. Such data security practices shall be appropriate to the volume and nature of the personal data at issue.
Other provisions	Nothing in this section shall apply to an individual or entity regulated by the State Corporation Commission’s Bureau of Insurance.

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	WASHINGTON (8/23)
Citation	Wash. Rev. Code §§ 19.255.005; 19.255.010; 19.255.040
Person Covered	Any person or business that conducts business in this state and that owns or licenses computerized data that includes personal information and any person or business that maintains computerized data that includes personal information that the person or business does not own.
Notification of Breach (Required)	Any person that owns or licenses computerized data that includes personal information shall disclose any breach to any affected resident whose unencrypted was or is reasonably believed to have been acquired by unauthorized persons. Any person that maintains or possesses data that may include personal information that the person does not own shall notify the owner or licensee of a breach if the information was or is reasonably believed to have been acquired by an unauthorized person and the personal information was not secured. Notification to affected consumers and to the attorney general must be made in the most expedient time possible and without unreasonable delay, no more than 30 days after breach was discovered. Any covered person shall also notify the attorney general if the entity is required to notify more than 500 Washington residents no more than 30 days after the breach is discovered.
Notification of Breach (Delay/Exemption)	Notification may be delayed if law enforcement determines notification will impede a criminal investigation.
Personal Information Defined (Encryption/Unencrypted)	"Personal information" means an individual's first name or first initial and last name in combination with another identifying data element. "Secured" means encrypted in a manner that meets or exceeds the national institute of standards and technology standard or is otherwise modified so that the personal information is rendered unreadable, unusable, or undecipherable by an unauthorized person. "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.
Breach of Security Defined	The unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith exception.
Penalties	Any consumer injured by a violation of this section may institute a civil action to recover damages. Violations of this section are an unfair or deceptive act in trade or commerce and an unfair method of competition for the purposes of applying the consumer protection act.
Private Cause of Action/Enforcement	Yes, enforcement by attorney general or individuals.
Safeguards	No provision
Other provisions	Any waiver of disclosure is contrary to public policy and is void and unenforceable.

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	WEST VIRGINIA (8/23)
Citation	§§ 46A-2A-101 to 46A-2A-105
Person Covered	An individual or entity that owns or licenses computerized data that includes personal information and an individual or entity that maintains computerized data that includes personal information that the individual or entity does not own or license.
Notification of Breach (Required)	Any entity that owns or licenses computerized data shall give notice of a breach to any affected resident whose unencrypted and unredacted information was or is reasonably believed to have been accessed by unauthorized persons that causes, or the person reasonably believes has caused, identity theft or fraud. Any entity that maintains computerized data that the entity does not own shall notify the owner or licensee if the personal information was or is reasonably believed to have been accessed by unauthorized persons. Notice shall be made without unreasonable delay. If a notification must be made to more than 1,000 persons, notification must be made to all consumer reporting agencies that files on a nationwide basis.
Notification of Breach (Delay/Exemption)	Notification may be delayed if law enforcement determines notification will impede a criminal investigation or jeopardize homeland or national security.
Personal Information Defined (Encryption/Unencrypted)	"Personal information" means the first name or first initial and last name linked to another identifying element in any form on an individual that is neither encrypted nor redacted. "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.
Breach of Security Defined	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 the state. Good faith exception.
Penalties	Violations constitute an unfair or deceptive act or practice. No civil penalty unless the court finds that the defendant has engaged in a course of repeated and willful violations of this article. No civil penalty shall exceed $150,000 per breach of security of the system or series of breaches of a similar nature that are discovered in a single investigation.
Private Cause of Action/Enforcement	No, enforcement by attorney general only. A violation of this article by a licensed financial institution shall be enforceable exclusively by the financial institution's primary or functional regulator.
Safeguards	No provision
Other provisions	

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	WISCONSIN (8/23)
Citation	§§ 134.97-134.98
Person Covered	If an entity whose principal place of business is located in this state or an entity that maintains or licenses personal information in this state and a person, other than an individual, that stores personal information pertaining to a resident of this state, but does not own or license the personal information.
Notification of Breach (Required)	Any covered person shall make reasonable efforts to notify the affected persons when the entity knows that the personal information has been acquired by unauthorized persons. Notification shall be within a reasonable time not to exceed 45 days after the entity learns of the acquisition of personal information. If an entity is required to notify more than 1,000 persons, the entity shall notify all consumer reporting agencies that maintain files on consumers on a nationwide basis.
Notification of Breach (Delay/Exemption)	Notification may be delayed upon a request by law enforcement if law enforcement determines notification will impede a criminal investigation or homeland security.
Personal Information Defined (Encryption/Unencrypted)	"Personal information" means an individual's last name and first name or first initial in combination with another identifying element that is not publicly available information and is not encrypted, redacted, or altered in a manner that renders the element unreadable. "Personal information" also includes: the individual's deoxyribonucleic acid profile; the individual's unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation. "Personal information" does not include: "publicly available information" which is any information that an entity reasonably believes is one of the following: lawfully made widely available through any media; lawfully made available to the general public from federal, state, or local government records or disclosures to the general public that are required to be made by federal, state, or local law.
Breach of Security Defined	No provision
Penalties	A financial institution, medical business, tax preparation business, or any person who possesses a record disposed of by one of the above listed entities may be fined or required to forfeit not more than $1,000 for each incident or occurrence.
Private Cause of Action/Enforcement	No, failure to comply with this section is not negligence or a breach of any duty, but may be evidence of negligence or a breach of a legal duty.
Safeguards	A financial institution, medical business, or tax preparation business shall take actions that it reasonably believes will ensure that no unauthorized person will have access to the personal information contained in the record for the period between the record's disposal and the record's destruction.
Other provisions	

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	WYOMING (8/23)
Citation	§§ 40-12-501 to 40-12-502; 6-3-901
Person Covered	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 and any person who maintains computerized data that includes personal identifying information on behalf of another business entity.
Notification of Breach (Required)	Any covered person shall, when they become aware of the breach, shall conduct a good faith investigation to determine the misuse of the personal information. If the investigation determines misuse, the entity shall give notice as soon as possible any affected state resident. Notice shall be made in the most expedient time possible and without unreasonable delay.
Notification of Breach (Delay/Exemption)	Notification may be delayed if law enforcement determines in writing that the notification may seriously impede a criminal investigation.
Personal Information Defined (Encryption/Unencrypted)	"Personal identifying information" means first name or first initial and last name of a person in combination with another identifying element and the data elements are not redacted. "Personal information" also includes: 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; 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 in widely distributed media that are lawfully made available to the general public.
Breach of Security Defined	Unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal identifying information by an employee or agent of a person or business for the purposes of the person or business and causes or is reasonably believed to cause loss or injury to a Wyoming resident. Good faith exception.

WYOMING (cont.)

GENERAL STATE PRIVACY BREACH/CONSUMER PROTECTION LAWS

	WYOMING (cont.)
Penalties	Actions in law or equity allowed to ensure proper compliance with this section, to recover damages, or both. Penalties for identity theft found in § 6-3-901.
Private Cause of Action/Enforcement	No, enforcement by attorney general only.
Safeguards	No provision
Other provisions	