Hintze Law PLLC

Privacy + Data Security

Hintze Law PLLC Condensed U.S. State Data Breach Notice Laws

Current through July 2023

The Hintze Cyber Security + Breach Response Group provides this document as a condensed, actionable guide of U.S. state data breach notification laws.

This document is organized into five sections. The Overview section, provides a high-level summary of the types of provisions that U.S. state data breach notification laws include. The next four sections, or Steps, are organized by and summarize the key requirements and information needed in connection with each stage of an incident. *Ctrl + click on the Steps to take you to that section.*

Step 1 - Is Notice Required?	Explores whether an incident requires notice. Types of personal information that are in-scope for the law. Types of incidents that count as a "breach." Key notice exceptions.
Step 2 - How and When to Notify Individuals?	Summarizes the requirements for providing notice to affected individuals. Includes deadlines and content requirements for notifications.
Step 3 - How and When Do I Notify Agencies?	Provides requirements for notifying state agencies like the state attorneys general and consumer reporting agencies. Includes deadlines and content requirements for these notifications.
Step 4 - What Are the Penalties?	Describes penalties for violations of the state data breach notice laws.

We encourage organizations experiencing a data breach to work with counsel to understand current laws and regulations relevant to the organization and incident to determine if notice is legally required and how notice should be provided.

This document does not represent a complete list of all laws that may apply in the event of a breach, nor does it detail all requirements in state data breach notification laws. In particular, this information does not address:

- *laws pertaining to obligations of government entities, insurance licensees, student data, electronic signature device managers, or data brokers that collect or maintain data to sell or transmit it to third parties*
- *federal laws such as HIPAA or GLBA*
- *supplementary laws that may apply to a subset of covered data or actors, such as financial account access information, telephone communication records, or motor vehicle dealerships*

Overview of U.S. State Breach Notice Laws

[Back to Introduction]

The District of Columbia, Guam, Puerto Rico, the U.S. Virgin Islands, and all U.S. states have laws requiring notice to data subjects about breaches of their sensitive personal information. The information below summarizes these data breach notice laws. We start with a brief summary of the similarities under these laws followed by a chart summarizing some of the key provisions that differ.

U.S. state data breach notice laws generally include the following elements:

Breach Trigger – The type of incident that can trigger notice obligations generally involves unauthorized acquisition of or access to personal information but can in other ways vary from state to state. Many states limit breach triggers to those involving "computerized" or electronic data. Some states require notice even if the data is not in electronic form. Some states only require notice if the security or confidentiality of personal information is materially compromised or there is harm. Others require notice for any unauthorized acquisition or access.

Definition of Personal Information - The definition of personal information varies from state to state but is generally limited to a first name or initial with a last name plus a type of sensitive information that if compromised can cause harm or identity theft, such as a Social Security Number, Driver's License Number, financial account number along with the PIN or password needed to access or use the account, or health or medical information. Some states include other types of personal information as data that can trigger a notice obligation when accompanied with an individual's name, such as biometric information, credit or debit card numbers, online account usernames and passwords, passport or other government identification information, or even more specific types of personal information. A number of states have notice obligations for some of the types of information noted above even if no name is involved.

Exceptions- There are several common exceptions to the definition of a breach or the obligation to give notice of a breach. For example:

- Where personal information is encrypted, redacted, or truncated, states generally have an exception or exclude such data from notice requirements. Some states, however, specifically state that the exception applies only so long as encryption has not been compromised (e.g., the encryption key has not been accessed without authorization).
- Where the incident does not impose a material risk of harm or identity theft on individuals, some states do not require affected individuals to be notified. Reliance on this exception sometimes requires state regulators to be notified that the entity suffering the breach is relying on this exception, and others require the entity to document this determination and maintain records of it for years.

- Most states do not require notification when the incident only resulted in unauthorized access or acquisition by an employee or agent acting in good faith, provided there was no further exposure or misuse of the personal information.
- Many states have exemptions to some of the notification requirements if notification of a breach is provided pursuant to other laws, such as HIPAA or GLBA.

Timing and Delay of Notice – Each state requires urgency in providing required notices. Some states require notice to be provided within a specific period of time after discovering the incident, but many simply require notice without unreasonable delay. States generally permit delay in notifying impacted individuals of a breach if an appropriate law enforcement agency determines that notification would interfere with a criminal investigation.

Notice to Individuals – All states require notice to residents in the event of a qualifying breach. The states vary with respect to contents of the notice; however, most states require notice to be in writing sent to the post address of the affected data subject. While most states only outline notification requirements for state residents, some states require notifications to be provided to all affected individuals even if those individuals are not state residents.

Attorney General/Regulatory Notice – Many states require notice to the state attorney general or another state government agency. Though not all states require such notice, many states mandate it and other states require it only in certain circumstances. States vary on the timing, content, and method of required notices to the attorney general or state government agency.

Notice to Consumer Reporting Agencies – Many states require notice to consumer reporting agencies if an organization will be notifying large numbers of individuals pursuant to the state law. States vary on what these numbers must be for a required notification to consumer reporting agencies.

Notice Requirements of Third-Party Vendors (and the like) – States generally require any party (such as a third-party vendor) that maintains information on behalf of a data owner or licensee to immediately notify the data owner or licensee of any in-scope data breach. Most states extend these obligations to breaches affecting nonresidents, requiring vendors to notify the data owner or licensee of every breach, even if resident information was not breached.

The charts below highlight major elements in the state breach notice laws that tend to differ from state to state. ***These charts are for informational purposes only and do not constitute legal advice or opinions.***

Step 1 – Is Notice Required?

[Back to Introduction]

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
Alabama Ala. Code §§ 8-38-1 – 8-38-9, 8-38-11 – 8-38-12 (Jun. 1, 2018)	"Sensitive personally identifying information…[means] an Alabama resident's first name or first initial and last name in combination with one or more of the following with respect to the same Alabama resident: 1. A non-truncated Social Security number or tax identification number. 2. A non-truncated driver's license number, state-issued identification card number, passport number, military identification number, or other unique identification number issued on a government document used to verify the identity of a specific individual. 3. A financial account number, including a bank account number, credit card number, or debit card number, in combination with any security code, access code, password, expiration date, or PIN, that is necessary to access the financial account or to conduct a transaction that will credit or debit the financial account. 4. Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional. 5. An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual. 6. A user name or email address, in combination with a password or security question and answer that would permit access to an online account affiliated with the covered entity that is reasonably likely to contain or is used to obtain sensitive personally identifying information." "[Sensitive personally identifying information] does not include either of the following:	"A covered entity that is not a third-party agent… determines that, as a result of a breach of security, sensitive personally identifying information has been acquired or is reasonably believed to have been acquired by an unauthorized person, and is reasonably likely to cause substantial harm to the individuals to whom the information relates." "[A] third-party agent has experienced a breach of security in the system maintained by the agent… [on behalf of] the covered entity." "[A covered entity] receiv[es] notice [of breach] from a third-party agent… [and there is no] contractual agreement with [the] third-party agent whereby the third-party agent agrees to handle [required] notifications." "In determining whether sensitive personally identifying information has been acquired or is reasonably believed to have been acquired by an unauthorized person without valid authorization, the following factors may be considered: (1) Indications that the information is in the physical possession and control of a person without valid authorization, such as a lost or stolen computer or other device containing information. (2) Indications that the information has been downloaded or copied. (3) Indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.	**Risk of harm threshold exception: Yes** **Encryption: Yes** *See Data Regulated* **Hard copy/paper format records in scope: No** **Good faith/agent exception: Yes** *See Triggering Event* **Exception if data was from public records: Yes** *See Data Regulated & Triggering Event* **Preempting law: Yes; more restrictive federal or state laws** "An entity subject to or regulated by federal [or state] laws, rules, regulations, procedures, or guidance on data breach notification established or enforced by the federal [or state] government is exempt from [duplicating already-required individual notice to satisfy this law's individual notice requirement] as long as the entity… [m]aintains procedures pursuant to those laws, rules, regulations, procedures, or guidance… [and] [p]rovides notice to affected individuals pursuant to those laws, rules, regulations, procedures, or guidance."

Step 1 - Is Notice Required?
[Back to Introduction]

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
	1. Information about an individual which has been lawfully made public by a federal, state, or local government record or a widely distributed media. 2. Information that is truncated, encrypted, secured, or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable, including encryption of the data, document, or device containing the sensitive personally identifying information, unless the covered entity knows or has reason to know that the encryption key or security credential that could render the personally identifying information readable or useable has been breached together with the information." "Individual… [means] [an] Alabama resident whose sensitive personally identifying information was, or the covered entity reasonably believes to have been, accessed as a result of the breach." "Data in electronic form… [means] data stored electronically or digitally on any computer system or other database, including, but not limited to, recordable tapes and other mass storage devices."	(4) Whether the information has been made public." "Breach of security or breach… [means] [t]he unauthorized acquisition of data in electronic form containing sensitive personally identifying information. Acquisition occurring over a period of time by the same entity constitutes one breach." "Breach of security or breach… [does not mean]: a. Good faith acquisition of sensitive personally identifying information by an employee or agent of a covered entity, unless the information is used for a purpose unrelated to the business or subject to further unauthorized use. b. The release of a public record not otherwise subject to confidentiality or nondisclosure requirements." "Covered entity… [means] [a] person, sole proprietorship, partnership… corporation, nonprofit, trust, estate, cooperative association, or other business entity that acquires or uses sensitive personally identifying information." "Third-party agent… [means] [a]n entity that has been contracted to maintain, store, process, or is otherwise permitted to access sensitive personally identifying information in connection with providing services to a covered entity."	**Exception recording: Yes** "If a covered entity determines that [individual] notice is not required… the entity shall document the determination in writing and maintain records concerning the determination for no less than five years." **Reliance on "no harm" exception requires AG notification: No**
Alaska	"'[P]ersonal information' means information in any form on an individual that is not encrypted or redacted, or is	"[A] covered person owns or licenses personal information in any form that includes personal	**Risk of harm threshold exception: Yes**

Step 1 - Is Notice Required?
[Back to Introduction]

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
Alaska Stat. §§ 45.48.010 – 45.48.090 (Jul. 1, 2009)	encrypted and the encryption key has been accessed or acquired, and that consists of a combination of (A) an individual's name… mean[ing] a combination of an individual's (i) first name or first initial; and (ii) last name; and (B) one or more of the following information elements: (i) the individual's social security number; (ii) the individual's driver's license number or state identification card number; (iii) except as provided in [the immediately below sub-sub-paragraph] (iv)… the individual's account number, credit card number, or debit card number; (iv) if an account can only be accessed with a personal code, the number in [the immediately above sub-sub-paragraph] (iii)… and the personal code… mean[ing] a security code, an access code, a personal identification number, or a password; (v) passwords, personal identification numbers, or other access codes for financial accounts."	information on a state resident, and a breach of the security of the information system that contains personal information occurs, [and] the covered person…discover[s] or…[is] notified of the breach." "'[B]reach of the security' means unauthorized acquisition, or reasonable belief of unauthorized acquisition, of personal information that compromises the security, confidentiality, or integrity of the personal information maintained by the information collector." "['Breach' does not include] the good faith acquisition of personal information by an employee or agent of an information collector for a legitimate purpose of the information collector… if the employee or agent does not use the personal information for a purpose unrelated to a legitimate purpose of the information collector and does not make further unauthorized disclosure of the personal information." "'[C]overed person' means a… person doing business… [or] person with more than 10 employees." "'[I]nformation 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." "[D]isclosure is not required if, after an appropriate investigation and after written	**Encryption exception: Yes** *See Data Regulated* **Hard copy/paper format records in scope: Yes** **Good faith/agent exception: Yes** *See Triggering Event* **Exception if data was from public records: Silent** **Preempting law: Yes; GLBA** "This section does not apply to an information collector who is subject to the Gramm-Leach-Bliley Financial Modernization Act." **Exception recording: Yes** "The determination [that breach notice to consumers is not required] shall be documented in writing, and the documentation shall be maintained for five years. *See Triggering Event* **Reliance on "no harm" exception requires AG notification: Yes** *See Triggering Event*

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
		notification to the attorney general of this state, 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. The determination shall be documented in writing, and the documentation shall be maintained for five years. The notification required by this subsection may not be considered a public record open to inspection by the public."	
Arizona Ariz. Rev. Stat. § 18-551, § 18-552 (Aug. 3, 2018; as amended Mar 29, 2022)	"'Personal information'… [means:] (i) An individual's first name or first initial and last name in combination with one or more specified data elements [defined below]. (ii) An individual's user name or e-mail address, in combination with a password or security question and answer, that allows access to an online account." "'Personal information'… [d]oes not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media." "'Individual' means a resident of this state who has a principal mailing address in this state as reflected in the records of the person conducting business in this state at the time of the breach." "'Specified data element' means any of the following: (a) An individual's social security number. (b) The number on an individual's driver license issued pursuant to [Ariz. Rev. Stat. § 28-3166] or nonoperating	"[A] person that conducts business in this state and that owns, maintains or licenses unencrypted and unredacted computerized personal information becomes aware of a security incident… determin[es] that there has been a security system breach." "'Breach' or 'security system breach'… [m]eans an unauthorized acquisition of and unauthorized access that materially compromises the security or confidentiality of unencrypted and unredacted computerized personal information maintained as part of a database of personal information regarding multiple individuals." "'Breach' or 'security system breach'… [d]oes not include a good faith acquisition of personal information by a person's employee or agent for the purposes of the person if the personal information is not used for a purpose unrelated to the person and is not subject to further unauthorized disclosure."	**Risk of harm threshold exception: Yes** **Encryption exception: Yes** *See Triggering Event* **Hard copy/paper format records in scope: No** **Good faith/agent exception: Yes** *See Triggering Event* **Exception if data was from public records: Yes** *See Data Regulated* **Preempting law: Yes; GLBA, HIPAA** "This [law] does not apply to either of the following: 1. A person that is subject to [15 U.S.C. §§ 6801 – 6809]. 2. A covered entity or business associates as defined under regulations implementing the health insurance portability and accountability act of 1996, [45 CFR

Step 1 - Is Notice Required?
[Back to Introduction]

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
	identification license issued pursuant to [Ariz. Rev. Stat. § 28-3165]. (c) A private key that is unique to an individual and that is used to authenticate or sign an electronic record. (d) An individual's financial account number or credit or debit card number in combination with any required security code, access code or password that would allow access to the individual's financial account. (e) An individual's health insurance identification number. (f) Information about an individual's medical or mental health treatment or diagnosis by a health care professional. (g) An individual's passport number. (h) An individual's taxpayer identification number or an identity protection personal identification number issued by the United States internal revenue service. (i) Unique biometric data generated from a measurement or analysis of human body characteristics to authenticate an individual when the individual accesses an online account."	"'Encrypt' means to use a process to transform data into a form that renders the data unreadable or unusable without using a confidential process or key." "'Person'… [m]eans a natural person, corporation, business trust, estate, trust, partnership, association, joint venture, government or governmental subdivision or agency or any other legal or commercial entity." "'Redact' means to alter or truncate a number so that not more than the last four digits are accessible and at least two digits have been removed." "'Security incident' means an event that creates reasonable suspicion that a person's information systems or computerized data may have been compromised or that measures put in place to protect the person's information systems or computerized data may have failed." "A person is not required to make the notification required by subsection B of this section if the person, an independent third-party forensic auditor or a law enforcement agency determines after a reasonable investigation that a security system breach has not resulted in or is not reasonably likely to result in substantial economic loss to affected individuals."	160.103] (2013) or a charitable fund-raising foundation or nonprofit corporation whose primary purpose is to support a specified covered entity, if the charitable fund-raising foundation or nonprofit corporation complies with any applicable provision of the health insurance portability and accountability act of 1996 and its implementing regulations." **Exception recording: No** **Reliance on "no harm" exception requires AG notification: No**

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
		"The person that maintains the data [unencrypted and unredacted computerized personal information that the person does not own or license] under an agreement with the owner or licensee is not required to provide the [individual] notifications… unless the agreement stipulates otherwise."	
Arkansas Ark. Code §§ 4-110-101 – 4-110-108 (Jul. 23, 2019)	"'Personal information' means an individual's first name or first initial and his or her last name in combination with any one (1) or more of the following data elements when either the name or the data element is not encrypted or redacted: (A) Social Security number; (B) Driver's license number or Arkansas identification card number; (C) Account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; (D) Medical information; and (E)(i) Biometric data. (ii) ['Biometric data']… means data generated by automatic measurements of an individual's biological characteristics, including without limitation: (a) Fingerprints; (b) Faceprint; (c) A retinal or iris scan; (d) Hand geometry; (e) Voiceprint analysis; (f) Deoxyribonucleic acid (DNA); or (g) Any other unique biological characteristics of an individual if the characteristics are used by the owner or	"A[] person or business that acquires, owns, or licenses computerized data that includes personal information… discover[s] or [is] notifi[ed] of the breach of the security of the system." "'Breach of the security of the system' means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person or business." "'Breach of the security of the system' does not include the good faith acquisition of personal information by an employee or agent of the person or business for the legitimate purposes of the person or business if the personal information is not otherwise used or subject to further unauthorized disclosure." "'Business' means a sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under	**Risk of harm threshold exception: Yes** **Encryption exception: Yes** *See Data Regulated* **Hard copy/paper format records in scope: No** *See Triggering Event* **Good faith/agent exception: Yes** *See Triggering Event* **Exception if data was from public records: Silent** **Preempting law: Yes; more restrictive federal or state laws.** "The provisions of this [law] do not apply to a person or business that is regulated by a state or federal law that provides greater protection to personal information and at least as thorough disclosure requirements for breaches of the security of personal information than that provided by [Ark. Code §§ 4-110-101 et seq.]" **Exception recording: Yes; retain in writing 5 years**

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
	licensee to uniquely authenticate the individual's identity when the individual accesses a system or account." "'Individual' means a natural person." "'Medical information' means any individually identifiable information, in electronic or physical form, regarding the individual's medical history or medical treatment or diagnosis by a healthcare professional."	the law of this state, any other state, the United States, or of any other country or the parent or the subsidiary of a financial institution… [and] includes… [a]n entity that destroys records." "'Owns or licenses' includes, but is not limited to… retain[ing] as part of the internal customer account of the business or for the purpose of using the information in transactions with the person to whom the information relates." "'Records' means any material that contains sensitive personal information in electronic form… [and] does not include any publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, such as name, address, or telephone number."	**Reliance on "no harm" exception requires AG notification: No** *However, AG can request exception recording*.
California Cal. Civ. Code § 1798.80, § 1798.82, § 1798.84, § 1798.150 (Jan. 1, 2021; § 1798.150 eff. Jan. 1, 2023)	"'Personal information' means either of the following: (1) An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (A) Social security number. (B) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual. (C) Account number or credit or debit card number, in combination with any required security code, access code,	"A person or business that conducts business in California, and that owns or licenses computerized data that includes personal information… discover[s] or [is] notifi[ed] of the breach in the security of the data [of] a resident of California (1) whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person, or, (2) whose encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person and the person or business that owns or licenses	**Risk of harm threshold exception: No** **Encryption exception: Yes** *See Data Regulated* **Hard copy/paper format records in scope: No** *See Triggering Event* **Good faith/agent exception: Yes** *See Triggering Event* **Exception if data was from public records: Silent** **Preempting law: Yes; HIPAA** (but only for individual notifications). **Exception recording: No**

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
	or password that would permit access to an individual's financial account. (D) Medical information. (E) Health insurance information. (F) Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes. (G) Information or data collected through the use or operation of an automated license plate recognition system, as defined in [Cal. Civ. Code § 1798.90.5(d)]. (2) A username or email address, in combination with a password or security question and answer that would permit access to an online account." "'[P]ersonal information' does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records." "'Individual' means a natural person." "'Records' means any material, regardless of the physical form, on which information is recorded or preserved by any means, including in written or spoken words, graphically depicted, printed, or electromagnetically transmitted… [and] does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, such as name, address, or telephone number."	the encrypted information has a reasonable belief that the encryption key or security credential could render that personal information readable or usable." "A person or business that maintains computerized data that includes personal information that the person or business does not own… discover[s]…the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." "'[B]reach of the security of the system' means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business." "[Breach of security does not include] [g]ood faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business… provided that the personal information is not used or subject to further unauthorized disclosure." "'Business' means a sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the law of this state, any other state, the United States, or of any other country, or the parent or	**Reliance on "no harm" exception requires AG notification: No**

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
		the subsidiary of a financial institution… [including] an entity that disposes of records." "'[E]ncryption key' and 'security credential' mean the confidential key or process designed to render data usable, readable, and decipherable."	
Colorado Colo. Rev. Stat. § 6-1-716 (Sep. 1, 2018)	"'Personal information' means a Colorado resident's first name or first initial and last name in combination with any one or more of the following data elements that relate to the resident, when the data elements are not encrypted, redacted, or secured by any other method rendering the name or the element unreadable or unusable: Social security number; student, military, or passport identification number; driver's license number or identification card number; medical information; health insurance identification number; or biometric data; (B) A Colorado resident's username or e-mail address, in combination with a password or security questions and answers, that would permit access to an online account; or (C) A Colorado resident's account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to that account." "[Personal information includes] encrypted or otherwise secured personal information… if the confidential process, encryption key, or other means to decipher the secured information was also acquired or was reasonably believed to have been acquired in the security breach."	"A covered entity… becomes aware that a security breach may have occurred, conduct[s] in good faith a prompt investigation to determine the likelihood that personal information has been or will be misused… [and does not] determine[] that the misuse of information about a Colorado resident has not occurred and is not reasonably likely to occur." "[A] covered entity uses a third-party service provider to maintain computerized data that includes personal information… discover[s]… a security breach… [and] misuse of personal information about a Colorado resident occurred or is likely to occur." "'Covered entity' means a person, as defined in [Colo. Rev. Stat. § 6-1-102(6)], that maintains, owns, or licenses personal information in the course of the person's business, vocation, or occupation. 'Covered entity' does not include a person acting as a third-party service provider as defined [below]." "'Security breach' means the unauthorized acquisition of unencrypted computerized data that	**Risk of harm threshold exception: Yes** **Encryption exception: Yes** *See Data Regulated* **Hard copy/paper format records in scope: No** *See Triggering Event* **Good faith/agent exception: Yes** *See Triggering Event* **Exception if data was from public records: Yes** *See Data Regulated* **Preempting law: Yes; compliance with other laws: HIPAA, GLBA** "A covered entity that is regulated by state or federal law and that maintains procedures for a security breach pursuant to the laws, rules, regulations, guidances, or guidelines established by its state or federal regulator is in compliance with this section; except that notice to the attorney general is still required pursuant to subsection (2)(f) of this section. In the case of a conflict between the

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
	"'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." "'Biometric data' means unique biometric data generated from measurements or analysis of human body characteristics for the purpose of authenticating the individual when he or she accesses an online account." "'Encrypted' means rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security." "'Medical information' means any information about a consumer's medical or mental health treatment or diagnosis by a health care professional."	compromises the security, confidentiality, or integrity of personal information maintained by a covered entity." "'Security breach… [does not include] good faith acquisition of personal information by an employee or agent of a covered entity for the covered entity's business purposes… if the personal information is not used for a purpose unrelated to the lawful operation of the business or is not subject to further unauthorized disclosure." "'Third-party service provider' means an entity that has been contracted to maintain, store, or process personal information on behalf of a covered entity."	time period for notice to individuals that is required pursuant to this subsection (3) and the applicable state or federal law or regulation, the law or regulation with the shortest time frame for notice to the individual controls." **Exception recording: No** **Reliance on "no harm" exception requires AG notification: No**
Connecticut Conn. Gen. Stat. § 36a-701b as amended by P.A. 21-59 (Oct. 1, 2021)	"'[P]ersonal information' means an individual's (A) first name or first initial and last name in combination with any one, or more, of the following data: (i) Social Security number; (ii) taxpayer identification number; (iii) identity protection personal identification number issued by the Internal Revenue Service; (iv) driver's license number, state identification card number, passport number, military identification number or other identification number issued by the government that is commonly used to verify identity; (v) credit or debit card number;	"[A] person who owns, licenses, or maintains computerized data that includes personal information…discover[s]…the breach." "[A] person that maintains computerized data that includes personal information that the person does not own…discover[s] [the breach]… [and] if the personal information of a resident of this state was breached or is reasonably believed to have been breached." "'[B]reach of security' means unauthorized access to or unauthorized acquisition of electronic files, media, databases or computerized data,	**Risk of harm threshold exception: Yes** **Encryption exception: Yes** *See Triggering Event* **Hard copy/paper format records in scope: No** *See Triggering Event* **Good faith/agent exception: Silent** **Exception if data was from public records: Yes** *See Data Regulated*

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
	(vi) financial account number in combination with any required security code, access code or password that would permit access to such financial account; (vii) medical information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; (viii) health insurance policy number or subscriber identification number, or any unique identifier used by a health insurer to identify the individual; or (ix) biometric information consisting of data generated by electronic measurements of an individual's unique physical characteristics used to authenticate or ascertain the individual's identity, such as a fingerprint, voice print, retina or iris image; or (B) user name or electronic 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 publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media."	containing personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable." "[Individual] notification shall not be required if, after an appropriate investigation the person reasonably determines the breach will not likely result in harm to the individuals whose personal information has been acquired or accessed."	**Preempting law: Yes; GLBA, HIPAA, more restrictive federal or state laws** "Any person that maintains such a security breach procedure pursuant to the rules, regulations, procedures or guidelines established by the primary or functional regulator, as defined in 15 USC 6809(2), shall be deemed to be in compliance with the security breach notification requirements of this section, provided (1) such person notifies, as applicable, such residents of this state, owners, and licensees required to be notified under and in accordance with the policies or the rules, regulations, procedures or guidelines established by the primary or functional regulator in the event of a breach of security, and (2) if notice is given to a resident of this state in accordance with subdivision (1) of this subsection regarding a breach of security, such person also notifies the Attorney General not later than the time when notice is provided to the resident." "Any person that is subject to and in compliance with the privacy and security standards under the Health Insurance Portability and

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
			Accountability Act of 1996 and the Health Information Technology for Economic and Clinical Health Act… shall be deemed to be in compliance with this section, provided that (1) any person required to provide notification to Connecticut residents pursuant to HITECH shall also provide notice to the Attorney General not later than the time when notice is provided to such residents if notification to the Attorney General would otherwise be required under subparagraph (A) of subdivision (2) of subsection (b) of this section, and (2) the person otherwise complies with the requirements of subparagraph (B) of subdivision (2) of subsection (b) of this section." **Exception recording: No** **Reliance on "no harm" exception requires AG notification: No**
Delaware Del. Code tit. 6 §§ 12B-101 – 12B-104 (Apr. 14, 2018)	"'Personal information' means a Delaware resident's first name or first initial and last name in combination with any 1 or more of the following data elements that relate to that individual: 1. Social Security number. 2. Driver's license number or state or federal identification card number.	"[A] person who conducts business in this State and who owns or licenses computerized data that includes personal information… [makes a] determination of the breach of security." "A person that maintains computerized data that includes personal information that the person	**Risk of harm threshold exception: Yes** **Encryption exception: Yes** *See Triggering Event* **Hard copy/paper format records in scope: No** *See Triggering Event* **Good faith/agent exception: Yes**

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
	3. Account number, credit card number, or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial account. 4. Passport number. 5. A username or email address, in combination with a password or security question and answer that would permit access to an online account. 6. Medical history, medical treatment by a health-care professional, diagnosis of mental or physical condition by a health-care professional, or deoxyribonucleic acid profile. 7. Health insurance policy number, subscriber identification number, or any other unique identifier used by a health insurer to identify the person. 8. Unique biometric data generated from measurements or analysis of human body characteristics for authentication purposes. 9. An individual taxpayer identification number." "'Personal information' does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely-distributed media."	does not own or license…[makes a] determination of the breach of security." "'Breach of security' means… [t]he unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information." "'Breach of security' [does not include] [g]ood faith acquisition of personal information by an employee or agent of any person for the purposes of such person… provided that the personal information is not used for an unauthorized purpose or subject to further unauthorized disclosure… [and also does not include] [t]he unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information… to the extent that personal information contained therein is encrypted, unless such unauthorized acquisition includes, or is reasonably believed to include, the encryption key and the person that owns or licenses the encrypted information has a reasonable belief that the encryption key could render that personal information readable or useable." "'Determination of the breach of security' means the point in time at which a person who owns, licenses, or maintains computerized data has sufficient evidence to conclude that a breach of security of such computerized data has taken place."	*See Triggering Event* **Exception if data was from public records: Yes** *See Data Regulated* **Preempting law: Yes; GLBA, HIPAA** "Under this chapter, a person that is regulated by state or federal law, including the Health Insurance Portability and Accountability Act of 1996 (P.L. 104-191, as amended) and the Gramm Leach Bliley Act (15 U.S.C. § 6801 et seq., as amended) and that maintains procedures for a breach of security pursuant to the laws, rules, regulations, guidance, or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance with this chapter if the person notifies affected Delaware residents in accordance with the maintained procedures when a breach of security occurs." **Exception recording: No** **Reliance on "no harm" exception requires AG notification: No**

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
		"'Encrypted' means personal information that is rendered unusable, unreadable, or indecipherable through a security technology or methodology generally accepted in the field of information security." "'Encryption key' means the confidential key or process designed to render the encrypted personal information useable, readable, and decipherable." "'Person' means an individual; corporation; business trust; estate trust; partnership; limited liability company; association; joint venture… public corporation; or any other legal or commercial entity."	
Florida Fla. Stat. § 501.171 (Oct. 1, 2019)	"'Personal information' means either of the following: a. An individual's first name or first initial and last name in combination with any one or more of the following data elements for that individual: (I) A social security number; (II) A driver license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity; (III) A financial account number or credit or debit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual's financial account; (IV) Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or	"[P]ersonal information was, or the covered entity reasonably believes to have been, accessed as a result of [a] breach." "In the event of a breach of security of a system maintained by a third-party agent." "'Breach of security' or 'breach' means unauthorized access of data in electronic form containing personal information." "'Breach of security' or 'breach'… [does not include] [g]ood faith access of personal information by an employee or agent of the covered entity… provided that the information is not used for a purpose unrelated to the business or subject to further unauthorized use."	**Risk of harm threshold exception: Yes** **Encryption exception: Yes** *See Data Regulated* **Hard copy/paper format records in scope: No** *See Triggering Event* **Good faith/agent exception: Yes** *See Triggering Event* **Exception if data was from public records: Yes** *See Data Regulated* **Preempting law: Yes; more restrictive federal or state laws** Notice provided pursuant to rules, regulations, procedures, or guidelines established by the covered entity's primary or

Step 1 - Is Notice Required?
[Back to Introduction]

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
	(V) An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual. b. A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account." "'Personal information'… does not include information about an individual that has been made publicly available by a federal, state, or local governmental entity. The term also does not include information that is encrypted, secured, or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable."	"'Covered entity' means a sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity that acquires, maintains, stores, or uses personal information." "'Data in electronic form' means any data stored electronically or digitally on any computer system or other database and includes recordable tapes and other mass storage devices." "'Third-party agent' means an entity that has been contracted to maintain, store, or process personal information on behalf of a covered entity."	functional federal regulator is deemed to be in compliance with the notice requirement in this subsection if the covered entity notifies affected individuals in accordance with the rules, regulations, procedures, or guidelines established by the primary or functional federal regulator in the event of a breach of security. Under this paragraph, a covered entity that timely provides a copy of such notice to the department is deemed to be in compliance with the notice requirement in subsection (3)." **Exception recording: Yes; maintained in writing for 5 years.** **Reliance on "no harm" exception requires AG notification: Yes; within 30 days of determination.**

Georgia Ga. Code § 10-1-911, § 10-1-912 (May 24, 2007)	"'Personal information' means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted: (A) Social security number; (B) Driver's license number or state identification card number; (C) Account number, credit card number, or debit card number, if circumstances exist wherein such a number could be used without additional identifying information, access codes, or passwords; (D) Account passwords or personal identification numbers or other access codes; or (E) Any of the items contained in [the immediately above] subparagraphs (A) through (D)… when not in connection with the individual's first name or first initial and last name, if the information compromised would be sufficient to perform or attempt to perform identity theft against the person whose information was compromised." "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."	"[An] information broker… that maintains computerized data that includes personal information of individuals…discover[s] or [is] notifi[ed] of [a] breach in the security of the data…[of] any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." "[A] person or business that maintains computerized data on behalf of an information broker… that includes personal information of individuals that the person or business does not own…discover[s] [the breach, and] the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." "'Breach of the security of the system' means unauthorized acquisition of an individual's electronic data that compromises the security, confidentiality, or integrity of personal information of such individual maintained by an information broker." "'Breach of the security of the system'… [does not include] [g]ood faith acquisition or use of personal information by an employee or agent of an information broker… for the purposes of such information broker… provided that the personal information is not used or subject to further unauthorized disclosure." "'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	**Risk of harm threshold exception: No** **Encryption exception: Yes** *See Data Regulated* **Hard copy/paper format records in scope: No** *See Triggering Event* **Good faith/agent exception: Yes** *See Triggering Event* **Exception if data was from public records: Yes** *See Data Regulated* **Preempting law: No** **Exception recording: No** **Reliance on "no harm" exception requires AG notification: No**

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
		furnishing personal information to nonaffiliated third parties." "'Person' means any individual, partnership, corporation, limited liability company, trust, estate, cooperative, association, or other entity… [and] shall not be construed to require duplicative reporting by any individual, corporation, trust, estate, cooperative, association, or other entity involved in the same transaction."	
Hawai'i Haw. Rev. Code §§ 487N-1 – 487N-3 (Jul. 1, 2008)	"'Personal information' means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social security number; (2) Driver's license number or Hawai'i identification card number; or (3) Account number, credit or debit card number, access code, or password that would permit access to an individual's financial account." "'Personal information' does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records." "'Encryption' or 'encrypted' means the use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without the use of a confidential process or key."	"A[] business that owns or licenses personal information of residents of Hawai'i, [or] a[] business that conducts business in Hawai'i that owns or licenses personal information in any form… discover[s] or [is] notifi[ed] of the breach." "[A] business located in Hawai'i or [a] business that conducts business in Hawai'i that maintains or possesses records or data containing personal information of residents of Hawai'i that the business does not own or license… discover[s] [the breach]." "'Business' means a sole proprietorship, partnership, corporation, association, or other group, however organized, and whether or not organized to operate at a profit… [including] a financial institution organized, chartered, or holding a license or authorization certificate under the laws of the State, any other state, the United States, or any other country, or the parent or the subsidiary of any such financial institution… [and	**Risk of harm threshold exception: Yes** **Encryption exception: Yes** *See Data Regulated* **Hard copy/paper format records in scope: Yes** *Triggering Event* **Good faith/agent exception: Yes** *See Triggering Event* **Exception if data was from public records: Yes** *See Data Regulated* **Preempting law: Yes; GLBA, HIPAA** "The following businesses shall be deemed to be in compliance with this section: 1) A financial institution that is subject to the federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice

Step 1 - Is Notice Required?
[Back to Introduction]

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
		including] an entity whose business is records destruction." "'Records' means any material on which written, drawn, spoken, visual, or electromagnetic information is recorded or preserved, regardless of physical form or characteristics." "'Redacted' means the rendering of data so that it is unreadable or is truncated so that no more than the last four digits of the identification number are accessible as part of the data." "'Security breach' means an incident of unauthorized access to and acquisition of unencrypted or unredacted records or data containing personal information where illegal use of the personal information has occurred, or is reasonably likely to occur and that creates a risk of harm to a person. 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." "'Security breach'… [does not include] [g]ood faith acquisition of personal information by an employee or agent of the business for a legitimate purpose… provided that the personal information is not used for a purpose other than a lawful purpose of the business and is not subject to further unauthorized disclosure."	published in the Federal Register on March 29, 2005, by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision, or subject to 12 C.F.R. Part 748, and any revisions, additions, or substitutions relating to the interagency guidance; and 2) Any health plan or healthcare provider that is subject to and in compliance with the standards for privacy or individually identifiable health information and the security standards for the protection of electronic health information of the Health Insurance Portability and Accountability Act of 1996." **Exception recording: No** **Reliance on "no harm" exception requires AG notification: No**

Step 1 - Is Notice Required?
[Back to Introduction]

Idaho Idaho Code §§ 28-51-104 – 28-51-107 (Jul. 1, 2015)	"'Personal information' means an Idaho resident's first name or first initial and last name in combination with any one (1) or more of the following data elements that relate to the resident, when either the name or the data elements are not encrypted: (a) Social security number; (b) Driver's license number or Idaho identification card number; or (c) Account number, or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial account." "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 or widely distributed media."	"[An] 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… becomes aware of a breach of the security of the system… [and] determines that the misuse of information about an Idaho resident has occurred or is reasonably likely to occur." "[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…discover[s] [a breach, and]… misuse of personal information about an Idaho resident occurred or is reasonably likely to occur." "'Breach of the security of the system' means the illegal acquisition of unencrypted computerized data that materially compromises the security, confidentiality, or integrity of personal information for one (1) or more persons maintained by an… individual or a commercial entity." "'Breach of the security of the system'… [does not include] [g]ood faith acquisition of personal information by an employee or agent of an… individual or a commercial entity for the purposes of the… individual or the commercial entity… provided that the personal information is not used or subject to further unauthorized disclosure." "'Commercial entity' includes corporation, business trust, estate, trust, partnership, limited partnership, limited liability partnership, limited liability company, association, organization, joint	**Risk of harm threshold exception: Yes** **Encryption exception: Yes** *See Data Regulated* **Hard copy/paper format records in scope: No** *See Triggering Event* **Good faith/agent exception: Yes** *See Triggering Event* **Exception if data was from public records: Yes** *See Data Regulated* **Preempting law: Yes; more restrictive federal or state laws** "a commercial entity that is regulated by state or federal law and that maintains procedures for a breach of the security of the system pursuant to the laws, rules, regulations, guidances, or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance with section 28-51-105, Idaho Code, if the individual or the commercial entity complies with the maintained procedures when a breach of the security of the system occurs." **Exception recording: No** **Reliance on "no harm" exception requires AG notification: No**

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
		venture and any other legal entity, whether for profit or not-for-profit."	

Step 1 - Is Notice Required?
[Back to Introduction]

Illinois 815 Ill. Comp. Stat. §§ 530/1 – 530/10, §§ 530/15 – 530/20 (Jan. 1, 2020)	"'Personal information' means either of the following: (1) An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the name or data elements have been acquired without authorization through the breach of security: (A) Social Security number. (B) Driver's license number or State identification card number. (C) Account number or credit or debit card number, or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account. (D) Medical information. (E) Health insurance information. (F) Unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee to authenticate an individual, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data. (2) User name or email address, in combination with a password or security question and answer that would permit access to an online account, when either the user name or email address or password or security question and answer are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the data elements have been obtained through the breach of security." "'Personal information' does not include publicly available information that is lawfully made available to the general public from federal, State, or local government records."	"[A] data collector that owns or licenses personal information concerning an Illinois resident…discover[s] or [is] notifi[ed] of the breach." "[A] 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…discover[s] [a breach]… [and] the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." "'Breach of the security of the system data' or 'breach' means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the data collector." "'Breach of the security of the system data' [or 'breach'] does not include good faith acquisition of personal information by an employee or agent of the data collector for a legitimate purpose of the data collector, provided that the personal information is not used for a purpose unrelated to the data collector's business or subject to further unauthorized disclosure." "'Data collector' may include, but is not limited to… 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."	**Risk of harm threshold exception: No** **Encryption exception: Yes** *See Data Regulated* **Hard copy/paper format records in scope: No** *See Triggering Event* **Good faith/agent exception: Yes** *See Triggering Event* **Exception if data was from public records: Yes** *See Data Regulated* **Preempting law: Yes; HIPAA** "This subsection does not apply to data collectors that are covered entities or business associates and are in compliance with Section 50." **Exception recording: No** **Reliance on "no harm" exception requires AG notification: No**

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
	"'Health insurance information' means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any medical information in an individual's health insurance application and claims history, including any appeals records. 'Medical information' means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional, including such information provided to a website or mobile application."		
Indiana Ind. Code §§ 24-4.9-1 – 24-4.9-5 (Jul. 1, 2017, as amended Mar. 18, 2022)	"'Personal information' means: (1) a Social Security number that is not encrypted or redacted; or (2) an individual's first and last names, or first initial and last name, and one (1) or more of the following data elements that are not encrypted or redacted: (A) A driver's license number. (B) A state identification card number. (C) A credit card number. (D) A financial account number or debit card number in combination with a security code, password, or access code that would permit access to the person's account." "[Personal information] does not include information that is lawfully obtained from publicly available information or from federal, state, or local government records lawfully made available to the general public." "Data are encrypted… if the data: (1) have been transformed through the use of an algorithmic process into a form in which there is a low	"[A data base owner] discover[s] or… [is] notified of a breach of the security of the data…[and] the data base owner knows, should know, or should have known that the unauthorized acquisition constituting the breach has resulted in or could result in identity deception… identity theft, or fraud affecting [the data subject]." "A person that maintains computerized data but… is not a data base owner… discovers that personal information was or may have been acquired by an unauthorized person." "'Breach of the security of data' means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person. The term includes the unauthorized acquisition of computerized data that have been transferred to another medium, including paper, microfilm, or a similar medium, even if the	**Risk of harm threshold exception: Yes** **Encryption exception: Yes** *See Data Regulated* **Hard copy/paper format records in scope: No** *See Triggering Event* **Good faith/agent exception: Yes** *See Triggering Event* **Exception if data was from public records: Yes** *See Data Regulated* **Preempting law: Yes; more restrictive federal or state laws:GLBA, HIPAA, FCRA, etc.** A data base owner that maintains its own disclosure procedures as part of an information privacy, security policy, or compliance plan under:

Step 1 - Is Notice Required?
[Back to Introduction]

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
	probability of assigning meaning without use of a confidential process or key; or (2) are secured by another method that renders the data unreadable or unusable." "Data are redacted… if the data have been altered or truncated so that not more than the last four (4) digits of: (1) a driver's license number; (2) a state identification number; or (3) an account number; is accessible as part of personal information." "[P]ersonal information is 'redacted' if the personal information has been altered or truncated so that not more than five (5) digits of a Social Security number are accessible as part of personal information."	transferred data are no longer in a computerized format." "[Breach of the security of data] does not include the following: (1) Good faith acquisition of personal information by an employee or agent of the person for lawful purposes of the person, if the personal information is not used or subject to further unauthorized disclosure. (2) Unauthorized acquisition of a portable electronic device on which personal information is stored, if all personal information on the device is protected by encryption and the encryption key: (A) has not been compromised or disclosed; and (B) is not in the possession of or known to the person who, without authorization, acquired or has access to the portable electronic device." "'Data base owner' means a person that owns or licenses computerized data that includes personal information." "'Doing business in Indiana' means owning or using the personal information of an Indiana resident for commercial purposes." "'Indiana resident' means a person whose principal mailing address is in Indiana, as reflected in records maintained by the data base owner." "'Person' means an individual, a corporation, a business trust, an estate, a trust, a partnership, an association, a nonprofit corporation or	(1) the federal USA PATRIOT Act (P.L. 107-56); (2) Executive Order 13224; (3) the federal Driver's Privacy Protection Act (18 U.S.C. 2781 et seq.); (4) the federal Fair Credit Reporting Act (15 U.S.C. 1681 et seq.); (5) the federal Financial Modernization Act of 1999 (15 U.S.C. 6801 et seq.); or (6) the federal Health Insurance Portability and Accountability Act (HIPAA) (P.L. 104-191); is not required to make a disclosure under this chapter if the data base owner's information privacy, security policy, or compliance plan requires that Indiana residents be notified of a breach of the security of data without unreasonable delay and the data base owner complies with the data base owner's information privacy, security policy, or compliance plan." **Exception recording: No** **Reliance on "no harm" exception requires AG notification: No**

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
		organization, a cooperative, or any other legal entity."	
Iowa Iowa Code §§ 715C.1 – 715C.2 (Jul. 1, 2018)	"'Personal information' means an individual's first name or first initial and last name in combination with any one or more of the following data elements that relate to the individual if any of the data elements are not encrypted, redacted, or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable or are encrypted, redacted, or otherwise altered by any method or technology but the keys to unencrypt, unredact, or otherwise read the data elements have been obtained through the breach of security: a. Social security number. b. Driver's license number or other unique identification number created or collected by a government body. c. Financial account number, credit card number, or debit card number in combination with any required expiration date, security code, access code, or password that would permit access to an individual's financial account. d. Unique electronic identifier or routing code, in combination with any required security code, access code, or password that would permit access to an individual's financial account. e. 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."	"[A] person who owns or licenses computerized data that includes a consumer's personal information that is used in the course of the person's business, vocation, occupation, or volunteer activities… discover[s]… [that information was subject to a] breach of security." "[A] person who maintains or otherwise possesses personal information on behalf of another person… discover[s]… [a] breach of security [wherein]… a consumer's personal information was included in the information that was breached." "'Breach of security' means unauthorized acquisition of personal information maintained in computerized form by a person that compromises the security, confidentiality, or integrity of the personal information. 'Breach of security' also means unauthorized acquisition of personal information maintained by a person in any medium, including on paper, that was transferred by the person to that medium from computerized form and that compromises the security, confidentiality, or integrity of the personal information." "['Breach of security' does not include] [g]ood faith acquisition of personal information by a person or that person's employee or agent for a legitimate	**Risk of harm threshold exception: Yes** **Encryption exception: Yes** *See Data Regulated* **Hard copy/paper format records in scope: No** *See Triggering Event* **Good faith/agent exception: Yes** *See Triggering Event* **Exception if data was from public records: Yes** *See Data Regulated* **Preempting law: Yes; GLBA, HIPAA, more restrictive federal or state laws** "This section does not apply to any of the following: a. A person who complies with notification requirements or breach of security procedures that provide greater protection to personal information and at least as thorough disclosure requirements than that provided by this section pursuant to the rules, regulations, procedures, guidance, or guidelines established by the person's primary or functional federal regulator.

Step 1 - Is Notice Required?
[Back to Introduction]

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
	"'Encryption' means the use of an algorithmic process pursuant to accepted industry standards to transform data into a form in which the data is rendered unreadable or unusable without the use of a confidential process or key." "'Redacted' means altered or truncated so that no more than five digits of a social security number or the last four digits of other numbers designated in [Iowa Code § 715A.8(1)(a)] are accessible as part of the data."	purpose of that person… provided that the personal information is not used in violation of applicable law or in a manner that harms or poses an actual threat to the security, confidentiality, or integrity of the personal information." "Notwithstanding subsection 1 [for notification], notification is not required if, after an appropriate investigation or after consultation with the relevant federal, state, or local agencies responsible for law enforcement, the person determined that no reasonable likelihood of financial harm to the consumers whose personal information has been acquired has resulted or will result from the breach. Such a determination must be documented in writing and the documentation must be maintained for five years." "'Consumer' means an individual who is a resident of this state." "'Person' means an individual; corporation; business trust; estate; trust; partnership; limited liability company; association; joint venture… public corporation; or any other legal or commercial entity."	b. A person who complies with a state or federal law that provides greater protection to personal information and at least as thorough disclosure requirements for breach of security or personal information than that provided by this section. c. A person who is subject to and complies with regulations promulgated pursuant to Tit. V of the federal Gramm-Leach-Bliley Act of 1999, 15 U.S.C. §6801 – 6809. d. A person who is subject to and complies with regulations promulgated pursuant to Tit. II, subtit. F of the federal Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. §1320d – 1320d-9, and Tit. XIII, subtit. D of the federal Health Information Technology for Economic and Clinical Health Act of 2009, 42 U.S.C. §17921 – 17954." **Exception recording: Yes; maintained in writing for 5 years. Reliance on "no harm" exception requires AG notification: No**
Kansas	"'Personal information' means a consumer's first name or first initial and last name linked to any one or more of the	"A person that conducts business in this state… that owns or licenses computerized data that	**Risk of harm threshold exception: Yes**

Step 1 - Is Notice Required?
[Back to Introduction]

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
Kan. Stat. §§ 50-7a01 – 50-7a02 (Jul. 1, 2006)	following data elements that relate to the consumer, when the data elements are neither encrypted nor redacted: (1) Social security number; (2) driver's license number or state identification card number; or (3) financial account number, or credit or debit card number, alone or in combination with any required security code, access code or password that would permit access to a consumer's financial account." "The term 'personal information' does not include publicly available information that is lawfully made available to the general public from federal, state or local government records." "'Consumer' means an individual who is a resident of this state." "'Encrypted' means transformation of data through the use of algorithmic process into a form in which there is a low probability of assigning meaning without the use of a confidential process or key, or securing the information by another method that renders the data elements unreadable or unusable." "'Redact' means alteration or truncation of data such that no more than the following are accessible as part of the personal information: (1) Five digits of a social security number; or (2) the last four digits of a driver's license number, state identification card number or account number."	includes personal information… becomes aware of any breach of the security of the system… determines that the misuse of information has occurred or is reasonably likely to occur." "An individual or commercial entity that maintains computerized data that includes personal information that the individual or the commercial entity does not own or license… discover[s]… a breach… [and] the personal information was, or is reasonably believed to have been, accessed and acquired by an unauthorized person." "'Person' means any individual, partnership, corporation, trust, estate, cooperative, association… or other entity." "'Security breach' means the unauthorized access and acquisition of unencrypted or unredacted computerized data that compromises the security, confidentiality or integrity of personal information maintained by an individual or a commercial entity and that causes, or such individual or entity reasonably believes has caused or will cause, identity theft to any consumer." "['Security breach' does not include] [g]ood faith acquisition of personal information by an employee or agent of an individual or a commercial entity for the purposes of the individual or the commercial entity… provided that the personal information is not used for or is not subject to further unauthorized disclosure."	**Encryption exception: Yes** *See Data Regulated* **Hard copy/paper format records in scope: No** *See Triggering Event* **Good faith/agent exception: Yes** *See Triggering Event* **Exception if data was from public records: Yes** *See Data Regulated* **Preempting law: Yes; more restrictive federal or state laws** "An individual or a commercial entity that is regulated by state or federal law and that maintains procedures for a breach of the security of the system pursuant to the laws, rules, regulations, guidances or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance with this section. This section does not relieve an individual or a commercial entity from a duty to comply with other requirements of state and federal law regarding the protection and privacy of personal information." **Exception recording: No** **Reliance on "no harm" exception requires AG notification: No**

Step 1 - Is Notice Required?
[Back to Introduction]

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
Kentucky Ky. Rev. Stat. § 365.732 (Jul. 15, 2014)	"'Personally identifiable information' means an individual's first name or first initial and last name in combination with any one (1) or more of the following data elements, when the name or data element is not redacted: 1. Social Security number; 2. Driver's license number; or 3. Account number or credit or debit card number, in combination with any required security code, access code, or password to permit access to an individual's financial account."	"[An] information holder…discover[s] or [is] notifi[ed] of the breach in the security of the data." "[An] information holder that maintains computerized data that includes personally identifiable information that the information holder does not own…discover[s] [the breach]… [and] the personally identifiable information was, or is reasonably believed to have been, acquired by an unauthorized person." "'Breach of the security of the system' means unauthorized acquisition of unencrypted and unredacted computerized data that compromises the security, confidentiality, or integrity of personally identifiable information maintained by the information holder as part of a database regarding multiple individuals that actually causes, or leads the information holder to reasonably believe has caused or will cause, identity theft or fraud against any resident of the Commonwealth of Kentucky." "[Breach of the security of the system does not include] [g]ood-faith acquisition of personally identifiable information by an employee or agent of the information holder for the purposes of the information holder… if the personally identifiable information is not used or subject to further unauthorized disclosure."	**Risk of harm threshold exception: Yes** **Encryption exception: Yes** *See Triggering Event* **Hard copy/paper format records in scope: No** *See Triggering Event* **Good faith/agent exception: Yes** *See Triggering Event* **Exception if data was from public records: Silent** **Preempting law: Yes; GLBA, HIPAA** *"The provisions of this section and the requirements for nonaffiliated third parties in KRS Chapter 61 shall not apply to any person who is subject to the provisions of Title V of the Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, as amended, or the federal Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, as amended, or any agency of the Commonwealth of Kentucky or any of its local governments or political subdivisions."* **Exception recording: No** **Reliance on "no harm" exception requires AG notification: No**

Step 1 - Is Notice Required?
[Back to Introduction]

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
		"'Information holder' means any person or business entity that conducts business in this state."	

Louisiana La. Rev. Stat. §§ 51:3071 – 51:3077 (Aug. 1, 2018) La. Admin. Code tit. 16, pt. III, § 701 (Mar. 20, 2007)	"'Personal information' means the first name or first initial and last name of an individual resident of this state in combination with any one or more of the following data elements, when the name or the data element is not encrypted or redacted: (i) Social security number. (ii) Driver's license number or state identification card number. (iii) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. (iv) Passport number. (v) Biometric data… mean[ing] data generated by automatic measurements of an individual's biological characteristics, such as fingerprints, voice print, eye retina or iris, or other unique biological characteristic that is used by the owner or licensee to uniquely authenticate an individual's identity when the individual accesses a system or account." "'Personal information' shall not include publicly available information that is lawfully made available to the general public from federal, state, or local government records."	"[A] person that conducts business in the state or that owns or licenses computerized data that includes personal information… discover[s]… a breach in the security of the system containing such data." "[A] person that maintains computerized data that includes personal information that the… person does not own… [and] the personal information was, or is reasonably believed to have been, acquired by an unauthorized person through a breach of security of the system containing such data… [and the person] discover[s]… [such breach]." "'Breach of the security of the system' means 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." "[Breach of the security of the system does not include] [g]ood faith acquisition of personal information by an employee or agent of an agency or person for the purposes of the agency or person… provided that the personal information is not used for, or is subject to, unauthorized disclosure." "'Person' means any individual, corporation, partnership, sole proprietorship, joint stock company, joint venture, or any other legal entity."	**Risk of harm threshold exception: Yes** **Encryption exception: Yes** *See Data Regulated* **Hard copy/paper format records in scope: No** *See Triggering Event* **Good faith/agent exception: Yes** *See Triggering Event* **Exception if data was from public records: Yes** *See Data Regulated* **Preempting law: Yes; GLBA** "A financial institution that is subject to and in compliance with the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, issued on March 7, 2005, by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the office of the comptroller of the currency and the office of thrift supervision, and any revisions, additions, or substitutions relating to said interagency guidance, shall be deemed to be in compliance with this Chapter." **Exception recording: Yes, for 5 years.** **Reliance on "no harm" exception requires AG notification: Yes, but only upon AG request.**

Step 1 - Is Notice Required?
[Back to Introduction]

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
Maine Me. Stat. tit. 10, §§ 1346 – 1350-A (Sep. 19, 2019)	"Personal information" means an individual's first name, or first initial, and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted: A. Social security number; B. Driver's license number or state identification card number; C. Account number, credit card number or debit card number, if circumstances exist wherein such a number could be used without additional identifying information, access codes or passwords; D. Account passwords or personal identification numbers or other access codes; or E. Any of the data elements contained in [the immediately above] paragraphs A to D when not in connection with the individual's first name, or first initial, and last name, if the information if compromised would be sufficient to permit a person to fraudulently assume or attempt to assume the identity of the person whose information was compromised." "'Personal information' does not include information from 3rd-party claims databases maintained by property and casualty insurers or publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media." "'Encryption' means the disguising of data using generally accepted practices."	"[A]n information broker that maintains computerized data that includes personal information becomes aware of a breach of the security of the system." "[Another] person who maintains computerized data that includes personal information becomes aware of a breach of the security of the system." "A 3rd-party entity that maintains, on behalf of a person, computerized data that includes personal information that the 3rd-party entity does not own…discover[s] [a breach]… [and] the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." "'Breach of the security of the system' or 'security breach' means 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." "['Breach of the security of the system' or 'security breach' does not include] [g]ood faith acquisition, release or use of personal information by an employee or agent of a person on behalf of the person… if the personal information is not used for or subject to further unauthorized disclosure to another person." "Information broker that maintains" or "any other person who maintains computerized data that	**Risk of harm threshold exception: Yes** **Encryption exception: Yes** *See Data Regulated* **Hard copy/paper format records in scope: No** **Good faith/agent exception: Yes** *See Triggering Event* **Exception if data was from public records: Yes** *See Data Regulated* **Preempting law: Yes; more restrictive federal or state laws** "A person that complies with the security breach notification requirements of rules, regulations, procedures or guidelines established pursuant to federal law or the law of this State is deemed to be in compliance with the requirements of section 1348 as long as the law, rules, regulations or guidelines provide for notification procedures at least as protective as the notification requirements of section 1348." **Exception recording: No** **Reliance on "no harm" exception requires AG notification: No**

Step 1 - Is Notice Required?
[Back to Introduction]

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
		includes personal information becomes aware of a breach of the security of the system" [they]... "shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused and shall give notice of a breach of the security of the system following discovery or notification of the security breach to a resident of this State if misuse of the personal information has occurred or if it is reasonably possible that misuse will occur." "'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 3rd parties." "'Person' means an individual, partnership, corporation, limited liability company, trust, estate, cooperative, association or other entity… [and] may not be construed to require duplicative notice by more than one individual, corporation, trust, estate, cooperative, association or other entity involved in the same transaction." "'System' means a computerized data storage system containing personal information." "'Unauthorized person' means a person who does not have authority or permission of a person	

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
		maintaining personal information to access personal information maintained by the person or who obtains access to such information by fraud, misrepresentation, subterfuge or similar deceptive practices."	
Maryland Md. Com. Law §§ 14-3501 – 14-3508 (Oct. 1, 2022)	"'Personal information' means: (i) An individual's first name or first initial and last name in combination with any one or more of the following data elements, when the name or the data elements are not encrypted, redacted, or otherwise protected by another method that renders the information unreadable or unusable: 1. A Social Security number, an Individual Taxpayer Identification Number, a passport number, or other identification number issued by the federal government; 2. A driver's license number or State identification card number; 3. An account number, a credit card number, or a debit card number, in combination with any required security code, access code, or password, that permits access to an individual's financial account; 4. Health information, including information about an individual's mental health; 5. A health insurance policy or certificate number or health insurance subscriber identification number, in combination with a unique identifier used by an insurer or an employer that is self-insured, that permits access to an individual's health information; 6. Biometric data of an individual generated by automatic measurements of an individual's biological characteristics such as a fingerprint, voice print, genetic print, retina or iris image, or other unique biological characteristic, that	"A business that owns, licenses, or maintains computerized data that includes personal information of an individual residing in the State… discovers or is notified that it incurred a breach of the security of a system, shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information of the individual has been or will be misused as a result of the breach… unless the business reasonably determines that the breach of the security of the system does not create a likelihood that personal information has been or will be misused, the owner or licensee of the computerized data shall notify the individual of the breach… If after the investigation… is concluded, the business determines that notification… is not required, the business shall maintain records that reflect its determination for 3 years after the determination is made." "A business that maintains computerized data that includes personal information of an individual residing in the State that the business does not own or license… discovers or is notified of a breach of the security of a system."	**Risk of harm threshold exception: Yes** **Encryption exception: Yes** *See Data Regulated* **Hard copy/paper format records in scope: No** **Good faith/agent exception: Yes** *See Triggering Event* **Exception if data was from public records: Yes** *See Data Regulated* **Preempting law: Yes; GLBA, HIPAA** "§ 14-3507. Compliance with federal laws... (b) A business that complies with the requirements for notification procedures, the protection or security of personal information, or the destruction of personal information under the rules, regulations, procedures, or guidelines established by the primary or functional federal or State regulator of the business

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
	can be used to uniquely authenticate the individual's identity when the individual accesses a system or account; or 7. For purposes of the notifications required under [this Act], genetic information with respect to an individual; (ii) A user name or e-mail address in combination with a password or security question and answer that permits access to an individual's e-mail account; or (iii) For the purposes of [this Act] other than the notifications required under [this Act], genetic information with respect to an individual when the genetic information is not encrypted, redacted, or otherwise protected by another method that renders the information unreadable or unusable, including: 1. Data, regardless of its format, that results from the analysis of a biological sample of the individual or from another source that enables equivalent information to be obtained and that concerns genetic material; 2. Deoxyribonucleic acids; 3. Ribonucleic acids; 4. Genes; 5. Chromosomes; 6. Alleles; 7. Genomes; 8. Alterations or modifications to deoxyribonucleic acids or ribonucleic acids; 9. Single nucleotide polymorphisms; 10. Uninterrupted data that results from the analysis of a biological sample from the individual or other sources; and 11. Information extrapolated, derived, or inferred from [items 1-10 of this list]." "'Personal Information' does not include:	"'Breach of the security system' means the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of the personal information maintained by a business." "'Breach of the security of a system' does not include the good faith acquisition of personal information by an employee or agent of a business for the purposes of the business, provided that the personal information is not used or subject to further unauthorized disclosure." "'Business' means a sole proprietorship, partnership, corporation, association, or any other business entity, whether or not organized to operate at a profit… [including] a financial institution organized, chartered, licensed, or otherwise authorized under the laws of this State, any other state, the United States, or any other country, and the parent or subsidiary of a financial institution."	shall be deemed to be in compliance with this subtitle. (c)(1) A business that is subject to and in compliance with § 501(b) of the federal Gramm-Leach-Bliley Act, 15 U.S.C. § 6801, § 216 of the federal Fair and Accurate Credit Transactions Act, 15 U.S.C. § 1681w, the federal Interagency Guidelines Establishing Information Security Standards, and the federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, and any revisions, additions, or substitutions, shall be deemed to be in compliance with this subtitle... (d)(1) A business that is subject to and in compliance with the federal Health Insurance Portability and Accountability Act of 1996 shall be deemed to be in compliance with this subtitle..." **Exception recording: Yes** **Reliance on "no harm" exception requires AG notification: No**

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
	(i) Publicly available information that is lawfully made available to the general public from federal, State, or local government records; (ii) Information that an individual has consented to have publicly disseminated or listed; or (iii) Information that is disseminated or listed in accordance with the federal Health Insurance Portability and Accountability Act." "'Encrypted' means the protection of data in electronic or optical form using an encryption technology that renders the data indecipherable without an associated cryptographic key necessary to enable decryption of the data." "'Health information' means any information created by an entity covered by the federal Health Insurance Portability and Accountability Act of 1996 regarding an individual's medical history, medical condition, or medical treatment or diagnosis."		
Massachusetts Mass. Gen. Laws §§ 93H-1 – 93H-6 (Apr. 10, 2019)	"'Personal information' [means] a resident's first name and last name or first initial and last name in combination with any 1 or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account."	"A person… that maintains or stores, but does not own or license data that includes personal information about a resident of the commonwealth… (1) knows or has reason to know of a breach of security or (2)… knows or has reason to know that the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose." "A person… that owns or licenses data that includes personal information about a resident of the commonwealth… (1) knows or has reason to	**Risk of harm threshold exception: No** **Encryption exception: Yes** *See Triggering Event* **Hard copy/paper format records in scope: Yes** **Good faith/agent exception: No** **Exception if data was from public records: Yes** *See Data Regulated* **Preempting law: Yes; more restrictive federal or state laws**

Step 1 - Is Notice Required?
[Back to Introduction]

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
	"'Personal information' shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public."	know of a breach of security or (2)… knows or has reason to know that the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose." "'Breach of security', [meaning] 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… that creates a substantial risk of identity theft or fraud against a resident of the commonwealth." "['Breach of security' does not include] good faith but unauthorized acquisition of personal information by a person… or employee or agent thereof, for the lawful purposes of such person… unless the personal information is used in an unauthorized manner or subject to further unauthorized disclosure." "'Encrypted' [means] transformation of data through the use of a 128-bit or higher algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key, unless further defined by regulation of the department of consumer affairs and business regulation." "'Data' [means] any material upon which written, drawn, spoken, visual, or electromagnetic	"[A] person who maintains procedures for responding to a breach of security pursuant to federal laws, rules, regulations, guidance, or guidelines, is deemed to be in compliance with this chapter if the person notifies affected Massachusetts residents in accordance with the maintained or required procedures when a breach occurs; provided further that the person also notifies the attorney general and the director of the office of consumer affairs and business regulation of the breach as soon as practicable and without unreasonable delay following the breach." **Exception recording: No** **Reliance on "no harm" exception requires AG notification: No**

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
		information or images are recorded or preserved, regardless of physical form or characteristics." "'Electronic' [means] relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities." "'Person' [means] a natural person, corporation, association, partnership or other legal entity."	
Michigan Mich. Comp. Laws §§ 445.61 – 445.64, § 445.72, § 445.72b (Jan. 1, 2020)	"'Personal information' means the first name or first initial and last name linked to 1 or more of the following data elements of a resident of this state: (i) Social security number. (ii) Driver license number or state personal identification card number. (iii) Demand deposit or other financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to any of the resident's financial accounts."	"[A] person… that owns or licenses data that are included in a database that discovers a security breach, or receives notice of a security breach [from a data licensee]." "[A] person… that maintains a database that includes data that the person… does not own or license… discovers a breach of the security of the database." "'Breach of the security of a database' or 'security breach' means the unauthorized access and acquisition of data that compromises the security or confidentiality of personal information maintained by a person… as part of a database of personal information regarding multiple individuals." "Unless the person or agency determines that the security breach has not or is not likely to cause substantial loss or injury to, or result in identity theft with respect to, 1 or more residents of this state. . ." notifications shall be provided. "In	**Risk of harm threshold exception: Yes** **Encryption exception: Yes** *See Triggering Event* **Hard copy/paper format records in scope: No** **Good faith/agent exception: Yes** *See Triggering Event* **Exception if data was from public records: Yes** "This section [12] does not apply to the access or acquisition by a person or agency of federal, state, or local government records or documents lawfully made available to the general public." **Preempting law: Yes; GLBA, HIPAA, more restrictive federal or state laws** "A financial institution that is subject to, and has notification procedures in place that are subject to examination by the

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
		determining whether a security breach is not likely to cause substantial loss or injury to, or result in identity theft with respect to, 1 or more residents of this state... a person or agency shall act with the care an ordinarily prudent person or agency in like position would exercise under similar circumstances." "['Breach of the security of database' or 'security breach' does not] include unauthorized access to data by an employee or other individual if the access meets all of the following: (i) The employee or other individual acted in good faith in accessing the data. (ii) The access was related to the activities of the agency or person. (iii) The employee or other individual did not misuse any personal information or disclose any personal information to an unauthorized person." "'Data' means computerized personal information." "'Encrypted' means transformation of data through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key, or securing information by another method that renders the data elements unreadable or unusable." "'Person' means an individual, partnership, corporation, limited liability company, association, or other legal entity."	financial institution's appropriate regulator for compliance with, the interagency guidance on response programs for unauthorized access to customer information and customer notice prescribed by the board of governors of the federal reserve system and the other federal bank and thrift regulatory agencies, or similar guidance prescribed and adopted by the national credit union administration, and its affiliates, is considered to be in compliance with this section." "A person or agency that is subject to and complies with the health insurance portability and accountability act of 1996, Public Law 104-191, and with regulations promulgated under that act, 45 CFR parts 160 and 164, for the prevention of unauthorized access to customer information and customer notice is considered to be in compliance with this section." "An entity that is subject to or regulated under… [Mich. Comp. Laws §§ 500.100 – 500.8302], is exempt from this [law]." "An entity that owns, is owned by, or is under common ownership with an entity [subject to or

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
		"'Redact' means to alter or truncate data so that no more than 4 sequential digits of a driver license number, state personal identification card number, or account number, or no more than 5 sequential digits of a social security number, are accessible as part of personal information."	regulated under Mich. Comp. Laws §§ 500.100 – 500.8302], and maintains the same cybersecurity procedures as that other entity, is exempt from this [law]." **Exception recording: No** **Reliance on "no harm" exception requires AG notification: No**
Minnesota Minn. Stat. § 325E.61 (Jul. 1, 2006)	"'[P]ersonal information' means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when the data element is not secured by encryption or another method of technology that makes electronic data unreadable or unusable, or was secured and the encryption key, password, or other means necessary for reading or using the data was also acquired: (1) Social Security number; (2) driver's license number or Minnesota identification card number; or (3) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account." "'[P]ersonal information' does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records."	"[A] person or business that conducts business in this state, and that owns or licenses data that includes personal information… discover[s] or [is] notifi[ed] of the breach in the security of the data." "[A] person or business that maintains data that includes personal information that the person or business does not own… discover[s] [a security breach]… [and] the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." "'Breach of the security of the system' means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business." "['Breach of the security of the system' does not include] [g]ood faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business… provided that the personal	**Risk of harm threshold exception: No** **Encryption exception: Yes** *See Data Regulated* **Hard copy/paper format records in scope: No** *See Triggering Event* **Good faith/agent exception: Yes** *See Triggering Event* **Exception if data was from public records: Yes** *See Data Regulated* **Preempting law: Yes; GLBA** "This [law]… do[es] not apply to any 'financial institution' as defined by [15 U.S.C. § 6809(3)]." **Exception recording: No** **Reliance on "no harm" exception requires AG notification: No**

Step 1 - Is Notice Required?
[Back to Introduction]

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
		information is not used or subject to further unauthorized disclosure."	
Mississippi Miss. Code § 75-24-29 (Jul. 1, 2021)	"'Personal information' means an individual's first name or first initial and last name in combination with any one or more of the following data elements: (i) Social security number; (ii) Driver's license number, state identification card number or tribal identification card number; or (iii) An account number or credit or debit card number in combination with any required security code, access code or password that would permit access to an individual's financial account." "'[P]ersonal 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."	"Notification shall not be required if, after an appropriate investigation, the person reasonably determines that the breach will not likely result in harm to the affected individuals.." "[A] person who conducts business in this state that maintains computerized data which includes personal information that the person does not own or license…discover[s] [a breach of security]… [and] the personal information was, or is reasonably believed to have been, acquired by an unauthorized person for fraudulent purposes." "'Breach of security' means unauthorized acquisition of electronic files, media, databases or computerized data containing personal information of any resident of this state when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable."	**Risk of harm threshold exception: Yes** **Encryption exception: Yes** *See Triggering Event* **Hard copy/paper format records in scope: No** *Triggering Event* **Court order exception: Silent** **Good faith/agent exception: No** **Exception if data was from public records: Yes** *See Data Regulated* **Preempting law: Yes; GLBA** "Any person that maintains such a security breach procedure pursuant to the rules, regulations, procedures or guidelines established by the primary or federal functional regulator, as defined in 15 USCS 6809(2), shall be deemed to be in compliance with the security breach notification requirements of this section, provided the person notifies affected individuals in accordance with the policies or the rules, regulations, procedures or guidelines established by the primary or federal functional

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
			regulator in the event of a breach of security of the system." **Exception recording: No** **Reliance on "no harm" exception requires AG notification: No**
Missouri Mo. Rev. Stat. § 407.1500 (Aug. 28, 2009)	"'Personal information', [meaning] an individual's first name or first initial and last name in combination with any one or more of the following data elements that relate to the individual if any of the data elements are not encrypted, redacted, or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable or unusable: (a) Social Security number; (b) Driver's license number or other unique identification number created or collected by a government body; (c) Financial account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; (d) Unique electronic identifier or routing code, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (e) Medical information; or (f) 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."	"A[] person that owns or licenses personal information of residents of Missouri or a[] person that conducts business in Missouri that owns or licenses personal information in any form of a resident of Missouri… discover[s] or [is] notifi[ed] of [a] breach." "A[] 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…discover[s]… [a] breach." "'Breach of security' or 'breach', [meaning] unauthorized access to and unauthorized acquisition of personal information maintained in computerized form by a person that compromises the security, confidentiality, or integrity of the personal information." "[N]otification is not required if, after an appropriate investigation by the person or after consultation with the relevant federal, state, or local agencies responsible for law enforcement,	**Risk of harm threshold exception: Yes** **Encryption exception: Yes** *See Data Regulated* **Hard copy/paper format records in scope: No** *See Triggering Event* **Good faith/agent exception: Yes** *See Triggering Event* **Exception if data was from public records: Yes** *See Data Regulated* **Preempting law: Yes; GLBA, more restrictive federal or state laws** "A person that is regulated by state or federal law and that maintains procedures for a breach of the security of the system pursuant to the laws, rules, regulations, guidances, or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance with this section if the person notifies affected consumers in accordance with the

Step 1 - Is Notice Required?
[Back to Introduction]

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
	"'Encryption' [means] the use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without the use of a confidential process or key." "'Health insurance information' [means] an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual." "'Medical information' [means] any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional." "'Redacted' [means] altered or truncated such that no more than five digits of a Social Security number or the last four digits of a driver's license number, state identification card number, or account number is accessible as part of the personal information."	the person determines that a risk of identity theft or other fraud to any consumer is not reasonably likely to occur as a result of the breach. Such a determination shall be documented in writing and the documentation shall be maintained for five years." "['Breach of security' or 'breach' does not include] [g]ood faith acquisition of personal information by a person or that person's employee or agent for a legitimate purpose of that person… provided that the personal information is not used in violation of applicable law or in a manner that harms or poses an actual threat to the security, confidentiality, or integrity of the personal information." "'Owns or licenses' includes, but is not limited to… retain[ing] as part of the internal customer account of the business or for the purpose of using the information in transactions with the person to whom the information relates." "'Person' [means] any individual, corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture… public corporation, or any other legal or commercial entity."	maintained procedures when a breach occurs." "A financial institution that is: (a) Subject to and in compliance with the Federal Interagency Guidance Response Programs for Unauthorized Access to Customer Information and Customer Notice, issued on March 29, 2005, by the board of governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision, and any revisions, additions, or substitutions relating to said interagency guidance; or (b) Subject to and in compliance with the National Credit Union Administration regulations in 12 CFR Part 748; or (c) Subject to and in compliance with the provisions of Title V of the Gramm-Leach-Bliley Financial Modernization Act of 1999, 15 U.S.C. Sections 6801 to 6809; shall be deemed to be in compliance with this section." **Exception recording: Yes; retain written recording for 5 years.** **Reliance on "no harm" exception requires AG notification: No**

Step 1 - Is Notice Required?
[Back to Introduction]

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
Montana Mont. Code § 30-14-1702, §§ 30-14-1704 – 30-14-1705 (Oct. 1, 2015)	"'Personal information' means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when the name and the data elements are not encrypted: (A) social security number; (B) driver's license number, state identification card number, or tribal identification card number; (C) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (D) medical record information as defined in [Mont. Code §] 33-19-104; (E) a taxpayer identification number; or (F) 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." "'Records' means any material, regardless of the physical form, on which personal information is recorded… [but] does not include publicly available directories containing personal information that an individual has voluntarily consented to have publicly disseminated or listed, such as name, address, or telephone number." "'Individual' means a natural person."	"[A] person or business that conducts business in Montana and that owns or licenses computerized data that includes personal information… discover[s] or [is] notifi[ed] of the breach." "[A] person or business that maintains computerized data that includes personal information that the person or business does not own…discover[s] [a breach]… [and] the personal information was or is reasonably believed to have been acquired by an unauthorized person." "'Breach of the security of the data system' means unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the person or business and causes or is reasonably believed to cause loss or injury to a Montana resident." "['Breach of the security of the data system' does not include] [g]ood faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business… provided that the personal information is not used or subject to further unauthorized disclosure." "'Business' means a sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under	**Risk of harm threshold exception: Yes** **Encryption exception: Yes** *See Data Regulated* **Hard copy/paper format records in scope: No** *See Triggering Event* **Good faith/agent exception: Yes** *See Triggering Event* **Exception if data was from public records: Yes** *See Data Regulated* **Preempting law: No** **Exception recording: No** **Reliance on "no harm" exception requires AG notification: No**

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
		the law of this state, any other state, the United States, or any other country or the parent or the subsidiary of a financial institution… [and] includ[ing] an entity that destroys records… [and] includ[ing] industries regulated by the public service commission or under [Mont. Code §§ 30-10-101 et seq.]… [but] not includ[ing] industries regulated under [Mont. Code §§ 33-1-101 et seq.]"	
Nebraska Neb. Rev. Stat. §§ 87-801 – 87-807 (Jul. 18, 2018)	"Personal information means either of the following: (a) a Nebraska resident's first name or first initial and last name in combination with any one or more of the following data elements that relate to the resident if either the name or the data elements are not encrypted, redacted, or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable: (i) Social security number; (ii) Motor vehicle operator's license number or state identification card number; (iii) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial account; (iv) Unique electronic identification number or routing code, in combination with any required security code, access code, or password; or (v) Unique biometric data, such as a fingerprint, voice print, or retina or iris image, or other unique physical representation. (b) A user name or email address, in combination with a password or security question and answer that would permit access to an online account."	"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 shall, when it becomes aware of a breach of the security of the system, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be used for an unauthorized purpose. If the investigation determines that the use of information about a Nebraska resident for an unauthorized purpose has occurred or is reasonably likely to occur, the individual or commercial entity shall give notice to the affected Nebraska resident.." "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 shall give notice to and cooperate with the owner or licensee of the information of any breach of the security of the system when it becomes aware of a breach if use of personal information about a	**Risk of harm threshold exception: Yes** **Encryption exception: Yes** *See Data Regulated* **Hard copy/paper format records in scope: No** *See Triggering Event* **Good faith/agent exception: Yes** *See Triggering Event* **Exception if data was from public records: Yes** *See Data Regulated* **Preempting law: Yes; more restrictive federal or state laws** "An individual or a commercial entity that is regulated by state or federal law and that maintains procedures for a breach of the security of the system pursuant to the laws, rules, regulations, guidances, or guidelines established by its primary or functional state or federal regulator is deemed to be in

Step 1 - Is Notice Required?
[Back to Introduction]

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
	"Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records." "Encrypted means converted by use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without use of a confidential process or key. Data shall not be considered encrypted if the confidential process or key was or is reasonably believed to have been acquired as a result of the breach of the security of the system." "Redact means to alter or truncate data such that no more than the last four digits of a social security number, motor vehicle operator's license number, state identification card number, or account number is accessible as part of the personal information."	Nebraska resident for an unauthorized purpose occurred or is reasonably likely to occur." "Breach of the security of the system means the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an individual or a commercial entity." "[Breach of the security of the system does not include] [g]ood faith acquisition of personal information by an employee or agent of an individual or a commercial entity for the purposes of the individual or the commercial entity…if the personal information is not used or subject to further unauthorized disclosure… [and does not include] [a]cquisition of personal information pursuant to a search warrant, subpoena, or other court order or pursuant to a subpoena or order of a state agency." "Commercial entity includes a corporation, business trust, estate, trust, partnership, limited partnership, limited liability partnership, limited liability company, association, organization, joint venture… or any other legal entity, whether for profit or not for profit."	compliance with section 87-803 if the individual or commercial entity notifies affected Nebraska residents and the Attorney General in accordance with the maintained procedures in the event of a breach of the security of the system." **Exception recording: No** **Reliance on "no harm" exception requires AG notification: No**
Nevada Nev. Rev. Stat. §§ 603A.010 – 603A.100, §§	"'Personal information' means a natural person's first name or first initial and last name in combination with any one or more of the following data elements, when the name and data elements are not encrypted:	"[A] data collector that owns or licenses computerized data which includes personal information…discover[s] or [is] notifi[ed] of the breach."	"The provisions of [this law]… do not apply to the maintenance or transmittal of information in accordance with [Nev. Rev. Stat.

Step 1 - Is Notice Required?
[Back to Introduction]

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
603A.215 – 603A.290 (Oct. 1, 2021)	(a) Social security number. (b) Driver's license number, driver authorization card number or identification card number. (c) Account number, credit card number or debit card number, in combination with any required security code, access code or password that would permit access to the person's financial account. (d) A medical identification number or health insurance identification number. (e) A user name, unique identifier or electronic mail address in combination with a password, access code or security question and answer that would permit access to an online account." "['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."	"[A] data collector that maintains computerized data which includes personal information that the data collector does not own… discover[s] [a breach, where]… the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." "'Breach of the security of the system data' means unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information maintained by the data collector." "['Breach of the security of the system data'] does not include the good faith acquisition of personal information by an employee or agent of the data collector for a legitimate purpose of the data collector, so long as the personal information is not used for a purpose unrelated to the data collector or subject to further unauthorized disclosure." "Data collector" means any… 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."	§§ 439.581 – 439.595], inclusive, and the regulations adopted pursuant thereto." **Risk of harm threshold exception: No** **Encryption exception: Yes** *See Data Regulated* **Hard copy/paper format records in scope: No** *See Triggering Event* **Good faith/agent exception: Yes** *See Triggering Event* **Exception if data was from public records: Yes** *See Data Regulated* **Preempting law: Yes; GLBA, more restrictive federal or state laws** "A data collector which: (a) Maintains its own notification policies and procedures as part of an information security policy for the treatment of personal information that is otherwise consistent with the timing requirements of this section shall be deemed to be in compliance with the notification requirements of this section if the data collector notifies subject persons in accordance with its policies and procedures in the event of a breach of the security of the system data.

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
			(b) Is subject to and complies with the privacy and security provisions of the Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801 et seq., shall be deemed to be in compliance with the notification requirements of this section." **Exception recording: No** **Reliance on "no harm" exception requires AG notification: No**
New Hampshire N.H. Rev. Stat. §§ 359-C:19 – 359-C:21 (Jan. 1, 2007)	"'Personal information' means an individual's first name or initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social security number. (2) Driver's license number or other government identification number. (3) Account number, credit card number, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account." "'Personal information' shall not include information that is lawfully made available to the general public from federal, state, or local government records." "'Encrypted' means the transformation of data through the use of an algorithmic process into a form for which there is a low probability of assigning meaning without use of a confidential process or key, or securing the information by another method that renders the data elements completely unreadable or unusable. Data shall	"Any person doing business in this state who owns or licenses computerized data that includes personal information shall, when it becomes aware of a security breach, promptly determine the likelihood that the information has been or will be misused. If the determination is that misuse of the information has occurred or is reasonably likely to occur, or if a determination cannot be made, the person shall notify the affected individuals as soon as possible..." "[A] person or business that maintains computerized data that includes personal information that the person or business does not own… discover[s] [a breach]… [and] the personal information was acquired by an unauthorized person." "'Computerized data' means personal information stored in an electronic format."	**Risk of harm threshold exception: Yes.** *See Triggering Event* **Encryption exception: Yes** *See Data Regulated* **Hard copy/paper format records in scope: No** *See Triggering Event* **Good faith/agent exception: Yes** **Exception if data was from public records: Yes** *See Data Regulated* **Preempting law: Yes; more restrictive federal or state laws** "Any person engaged in trade or commerce that is subject to RSA 358-A:3, I which maintains procedures for security breach notification pursuant to the laws, rules, regulations, guidances, or guidelines issued by a state or federal regulator shall be deemed

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
	not be considered to be encrypted… if it is acquired in combination with any required key, security code, access code, or password that would permit access to the encrypted data."	"'Security breach' means unauthorized acquisition of computerized data that compromises the security or confidentiality of personal information maintained by a person doing business in this state." "['Security breach' does not include] [g]ood faith acquisition of personal information by an employee or agent of a person for the purposes of the person's business… provided that the personal information is not used or subject to further unauthorized disclosure." "'Person' means an individual, corporation, trust, partnership, incorporated or unincorporated association, limited liability company, or other form of entity."	to be in compliance with this subdivision if it acts in accordance with such laws, rules, regulations, guidances, or guidelines." **Exception recording: No** **Reliance on "no harm" exception requires AG notification: No**
New Jersey N.J. Stat. § 56:8-161, § 56:8-163, §§ 56:8-165 – 56:8-166 (Sep. 1, 2019)	"'Personal information' means an individual's first name or first initial and last name linked with any one or more of the following data elements: (1) Social Security number; (2) driver's license number or State identification card number; or (3) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. Dissociated data that, if linked, would constitute personal information is personal information if the means to link the dissociated data were accessed in connection with access to the dissociated data."	"[A] business that conducts business in New Jersey… discover[s] or [is] notifi[ed] of the breach." "[A] business… that compiles or maintains computerized records that include personal information on behalf of another business or public entity… discover[s] [a breach]… [and] the personal information was, or is reasonably believed to have been, accessed by an unauthorized person." "'Breach of security' means unauthorized access to electronic files, media or data containing personal information that compromises the security, confidentiality or integrity of personal information	**Risk of harm threshold exception: Yes** "Disclosure of a breach of security to a customer shall not be required under this section if the business or public entity establishes that misuse of the information is not reasonably possible." **Encryption exception: Yes** *See Triggering Event* **Hard copy/paper format records in scope: No** *See Triggering Event* **Good faith/agent exception: Yes**

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
	"[P]ersonal information shall not include publicly available information that is lawfully made available to the general public from federal, state or local government records, or widely distributed media." "'Individual' means a natural person."	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." "['Breach of security' does not include] [g]ood faith acquisition of personal information by an employee or agent of the business for a legitimate business purpose… provided that the personal information is not used for a purpose unrelated to the business or subject to further unauthorized disclosure." "'Business' means a sole proprietorship, partnership, corporation, association, or other entity, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the law of this State, any other state, the United States, or of any other country, or the parent or the subsidiary of a financial institution."	*See Triggering Event* **Exception if data was from public records: Yes** *See Data Regulated* **Preempting law: No** "a business or public entity that maintains its own notification procedures as part of an information security policy for the treatment of personal information, and is otherwise consistent with the requirements of this section, shall be deemed to be in compliance with the notification requirements of this section if the business or public entity notifies subject customers in accordance with its policies in the event of a breach of security of the system." **Exception recording: Yes** "Any determination [that misuse of information is not reasonably possible] shall be documented in writing and retained for five years." **Reliance on "no harm" exception requires AG notification: No**

New Mexico N.M. Stat. §§ 57-12C-1 – 57-12C-2, §§ 57-12C-6 – 57-12C-11 (Jun. 16, 2017)	"'[P]ersonal identifying information': (1) 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: (a) social security number; (b) driver's license number; (c) government-issued identification number; (d) account number, credit card number or debit card number in combination with any required security code, access code or password that would permit access to a person's financial account; or (e) biometric data." "['Personal identifying information'] does not mean information that is lawfully obtained from publicly available sources or from federal, state or local government records lawfully made available to the general public." "'[B]iometric data' means a record generated by automatic measurements of an identified individual's fingerprints, voice print, iris or retina patterns, facial characteristics or hand geometry that is used to uniquely and durably authenticate an individual's identity when the individual accesses a physical location, device, system or account." "'[E]ncrypted' means rendered unusable, unreadable or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security."	"[A] person that owns or licenses elements that include personal identifying information of a New Mexico resident… discover[s]… the security breach." "[A] 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… discover[s]… the breach." "'[S]ecurity breach' means the unauthorized acquisition of unencrypted computerized data, or of encrypted computerized data and the confidential process or key used to decrypt the encrypted computerized data, that compromises the security, confidentiality or integrity of personal identifying information maintained by a person." "'Security breach' does not include the good-faith acquisition of personal identifying information by an employee or agent of a person for a legitimate business purpose of the person; provided that the personal identifying information is not subject to further unauthorized disclosure."	**Risk of harm threshold exception: Yes** "[N]otification to affected New Mexico residents is not required if, after an appropriate investigation, the person determines that the security breach does not give rise to a significant risk of identity theft or fraud." "[N]otification to the owner or licensee of the information is not required if, after an appropriate investigation, the person determines that the security breach does not give rise to a significant risk of identity theft or fraud." **Encryption exception: Yes** *See Data Regulated* **Hard copy/paper format records in scope: No** *See Triggering Event* **Good faith/agent exception: Yes** *See Triggering Event* **Exception if data was from public records: Yes** *See Data Regulated* **Preempting law: Yes; GLBA, HIPAA** "The provisions of [this law] shall not apply to a person subject to the federal Gramm-Leach-Bliley Act or the federal Health Insurance Portability and Accountability Act of 1996." **Exception recording: No**

Step 1 - Is Notice Required?
[Back to Introduction]

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
			Reliance on "no harm" exception requires AG notification: No
New York N.Y. Gen. Bus. Law § 899-AA (Oct. 23, 2019)	"'Personal information' shall mean any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person." "'Private information' shall mean either: (i) personal information consisting of any information in combination with any one or more of the following data elements, when either the data element or the combination of personal information plus the data element is not encrypted, or is encrypted with an encryption key that has also been accessed or acquired: (1) social security number; (2) driver's license number or non-driver identification card number; (3) account number, credit or debit card number, in combination with any required security code, access code, password or other information that would permit access to an individual's financial account; (4) account number, credit or debit card number, if circumstances exist wherein such number could be used to access an individual's financial account without additional identifying information, security code, access code, or password; or (5) biometric information, meaning data generated by electronic measurements of an individual's unique physical characteristics, such as a fingerprint, voice print, retina or iris image, or other unique physical representation or digital representation of biometric data	"[A] person or business which owns or licenses computerized data which includes private information… discover[s] or [is] notifi[ed] of the breach in the security of the system." "[A] person or business which maintains computerized data which includes private information which such person or business does not own… discover[s] [a security breach].. [and] the private information was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization." "'Breach of the security of the system' shall mean unauthorized access to or acquisition of, or access to or acquisition without valid authorization, of computerized data that compromises the security, confidentiality, or integrity of private information maintained by a business." "['Breach of the security of the system' does not include] [g]ood faith access to, or acquisition of, private information by an employee or agent of the business for the purposes of the business… provided that the private information is not used or subject to unauthorized disclosure." "In determining whether information has been accessed, or is reasonably believed to have been accessed, by an unauthorized person or a person	**Risk of harm threshold exception: Yes** "Notice to affected persons under this section is not required if the exposure of private information was an inadvertent disclosure by persons authorized to access private information, and the person or business reasonably determines such exposure will not likely result in misuse of such information, or financial harm to the affected persons or emotional harm in the case of unknown disclosure of online credentials..." **Encryption exception: Yes** *See Data Regulated* **Hard copy/paper format records in scope: No** *See Triggering Event* **Good faith/agent exception: Yes** *See Triggering Event* **Exception if data was from public records: Yes** *See Data Regulated* **Preempting law: Yes; HIPAA, GLBA, more restrictive federal or state laws** If notice of the breach of the security of the system is made to

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
	which are used to authenticate or ascertain the individual's identity; or (ii) a user name or e-mail address in combination with a password or security question and answer that would permit access to an online account." "'Private information' does not include publicly available information which is lawfully made available to the general public from federal, state, or local government records."	without valid authorization, such business may consider, among other factors, indications that the information was viewed, communicated with, used, or altered by a person without valid authorization or by an unauthorized person. In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization, such business may consider the following factors, among others: (1) indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information; or (2) indications that the information has been downloaded or copied; or (3) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported."	affected persons pursuant to the breach notification requirements under any of the following laws, nothing in this section shall require any additional notice to those affected persons, but notice still shall be provided to the state attorney general, the department of state and the division of state police pursuant to paragraph (a) of subdivision eight of this section and to consumer reporting agencies pursuant to paragraph (b) of subdivision eight of this section: (i) regulations promulgated pursuant to Title V of the federal Gramm-Leach-Bliley Act (15 U.S.C. 6801 to 6809), as amended from time to time; (ii) regulations implementing the Health Insurance Portability and Accountability Act of 1996 (45 C.F.R. parts 160 and 164), as amended from time to time, and the Health Information Technology for Economic and Clinical Health Act, as amended from time to time; (iii) part five hundred of title twenty-three of the official compilation of codes, rules and regulations of the state of New York, as amended from time to time; or

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
			(iv) any other data security rules and regulations of, and the statutes administered by, any official department, division, commission or agency of the federal or New York state government as such rules, regulations or statutes are interpreted by such department, division, commission or agency or by the federal or New York state courts. **Exception recording: Yes; retain in writing for 5 years.** **Reliance on "no harm" exception requires AG notification: Yes, notify AG within 10 days after determination of "no harm" if incident affects >500** "Such a determination must be documented in writing and maintained for at least five years. If the incident affects over five hundred residents of New York, the person or business shall provide the written determination to the state attorney general within ten days after the determination."
North Carolina	"'Personal information'… [means a] person's first name or first initial and last name in combination with identifying	"[A] business that owns or licenses personal information of residents of North Carolina or any business that conducts business in North Carolina	**Risk of harm threshold exception: Yes** **Encryption exception: Yes**

Step 1 - Is Notice Required?
[Back to Introduction]

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
N.C. Gen. Stat. § 75-60, § 75-61, § 75-65 (Jan. 1, 2016)	information as defined in [N.C. Gen. Stat. §] 14-113.20(b)." "'[I]dentifying information' as used in [N.C. Gen. Stat. §§ 14-113.20 et seq.] includes the following: (1) Social security or employer taxpayer identification numbers. (2) Driver's license, State identification card, or passport numbers. (3) Checking account numbers. (4) Savings account numbers. (5) Credit card numbers. (6) Debit card numbers. (7) Personal Identification (PIN) Code as defined in [N.C. Gen. Stat. §] 14-113.8(6). (8) Electronic identification numbers, electronic mail names or addresses, Internet account numbers, or Internet identification names. (9) Digital signatures. (10) Any other numbers or information that can be used to access a person's financial resources. (11) Biometric data. (12) Fingerprints. (13) Passwords. (14) Parent's legal surname prior to marriage." "[In N.C. Gen. Stat. §§ 14-1 et seq.,] '[p]ersonal identification code' means a numeric and/or alphabetical code assigned to the cardholder of a financial transaction card by the issuer to permit authorized electric use of that [financial transaction card]." "Personal information does not include publicly available directories containing information an individual has	that owns or licenses personal information in any form (whether computerized, paper, or otherwise)… discover[s] or [is] notifi[ed] of… [a] breach." "[A] 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…discover[s]… [a] breach." "'Business'… [means] [a] sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not organized to operate at a profit… [including] a financial institution organized, chartered, or holding a license or authorization certificate under the laws of this State, any other state, the United States, or any other country, or the parent or the subsidiary of any such financial institution." "'Encryption'… [means] [t]he use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without use of a confidential process or key." "'Person'… [means an] individual, partnership, corporation, trust, estate, cooperative, association… or other entity."	*See Triggering Event* **Hard copy/paper format records in scope: Yes** *See Triggering Event* **Good faith/agent exception: Yes** *See Triggering Event* **Exception if data was from public records: Yes** *See Data Regulated* **Preempting law: Yes; more restrictive federal or state laws** "A financial institution that is subject to and in compliance with the Federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice, issued on March 7, 2005, by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision; or a credit union that is subject to and in compliance with the Final Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice, issued on April 14, 2005, by the National Credit Union Administration; and any revisions, additions, or substitutions relating to any of the said interagency

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
	voluntarily consented to have publicly disseminated or listed, including name, address, and telephone number, and does not include information made lawfully available to the general public from federal, state, or local government records." "[P]ersonal information shall not include electronic identification numbers, electronic mail names or addresses, Internet account numbers, Internet identification names, parent's legal surname prior to marriage, or a password… [if such] information would [not] permit access to a person's financial account or resources."	"'Records'… [means] [a]ny material on which written, drawn, spoken, visual, or electromagnetic information is recorded or preserved, regardless of physical form or characteristics." "'Redaction'… [means] [t]he rendering of data so that it is unreadable or is truncated so that no more than the last four digits of the identification number is accessible as part of the data." "'Security breach'… [means an] incident of unauthorized access to and acquisition of unencrypted and unredacted records or data containing personal information where illegal use of the personal information has occurred or is reasonably likely to occur or that creates a material risk of harm to a consumer. Any incident of unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential process or key shall constitute a security breach." "['Security breach' does not include] [g]ood faith acquisition of personal information by an employee or agent of the business for a legitimate purpose… provided that the personal information is not used for a purpose other than a lawful purpose of the business and is not subject to further unauthorized disclosure."	guidance, shall be deemed to be in compliance with this section." **Exception recording: No** **Reliance on "no harm" exception requires AG notification: No**
North Dakota	"'Personal information' means an individual's first name or first initial and last name in combination with any of	"[A] person that owns or licenses computerized data that includes personal	**Risk of harm threshold exception: No** **Encryption exception: Yes**

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
N.D. Cent. Code §§ 51-30-01 – 51-30-07 (Aug. 1, 2015)	the following data elements, when the name and the data elements are not encrypted: (1) The individual's social security number; (2) The operator's license number assigned to an individual by the department of transportation under [N.D. Cent. Code §] 39-06-14; (3) A nondriver color photo identification card number assigned to the individual by the department of transportation under [N.D. Cent. Code §] 39-06-03.1; (4) The individual's financial institution account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial accounts; (5) The individual's date of birth; (6) The maiden name of the individual's mother; (7) Medical information; (8) Health insurance information; (9) An identification number assigned to the individual by the individual's employer in combination with any required security code, access code, or password; or (10) 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." "'Health insurance information' means an individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual."	information…discover[s] or [is] notifi[ed] of… [a] breach in the security of the data." "[A] person that maintains computerized data that includes personal information that the person does not own… discover[s] [a breach]… [and] the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." "'Breach of the security system' means unauthorized acquisition of computerized data when access to personal information has not been secured by encryption or by any other method or technology that renders the electronic files, media, or databases unreadable or unusable." "['Breach of the security system' does not include] [g]ood-faith acquisition of personal information by an employee or agent of the person… if the personal information is not used or subject to further unauthorized disclosure."	*See Data Regulated* **Hard copy/paper format records in scope: No** *See Triggering Event* **Good faith/agent exception: Yes** *See Triggering Event* **Exception if data was from public records: Yes** *See Data Regulated* **Preempting law: Yes; GLBA, HIPAA, more restrictive federal or state laws** "Notwithstanding section 51-30-05, a person that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this chapter is deemed to be in compliance with the notification requirements of this chapter if the person notifies subject individuals in accordance with its policies in the event of a breach of security of the system. A financial institution, trust company, or credit union that is subject to, examined for, and in compliance with the federal interagency guidance on response programs for unauthorized access to customer information and customer notice is in compliance

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
	"'Medical information' means any information regarding an individuals' medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional."		with this chapter. A covered entity, business associate, or subcontractor subject to breach notification requirements under title 45, Code of Federal Regulations, subpart D, part 164, is considered to be in compliance with this chapter." **Exception recording: No** **Reliance on "no harm" exception requires AG notification: No**

Ohio Ohio Rev. Code §§ 1349.19 – 1349.192 (Mar. 30, 2007)	"'Personal information' means an individual's name, consisting of the individual's first name or first initial and last name, in combination with and linked to any one or more of the following data elements, when the data elements are not encrypted, redacted, or altered by any method or technology in such a manner that the data elements are unreadable: (i) Social security number; (ii) Driver's license number or state identification card number; (iii) Account number or credit or debit card number, in combination with and linked to any required security code, access code, or password that would permit access to an individual's financial account." "'Personal information' does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or any of the following media that are widely distributed: (i) Any news, editorial, or advertising statement published in any bona fide newspaper, journal, or magazine, or broadcast over radio or television; (ii) Any gathering or furnishing of information or news by any bona fide reporter, correspondent, or news bureau to news media described in [the immediately above paragraph]; (iii) Any publication designed for and distributed to members of any bona fide association or charitable or fraternal nonprofit corporation; (iv) Any type of media similar in nature to any item, entity, or activity identified in [the three immediately above paragraphs]." "'Encryption' means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key."	"[A] person that owns or licenses computerized data that includes personal information… discover[s] or [is] notifi[ed] of the breach of the security of the system." "[A] person that, on behalf of or at the direction of another person… is the custodian of or stores computerized data that includes personal information… [that] was, or reasonably is believed to have been, accessed and acquired by an unauthorized person and… the access and acquisition by the unauthorized person causes or reasonably is believed will cause a material risk of identity theft or other fraud to a resident of this state." "'Breach of the security of the system' means unauthorized access to and acquisition of computerized data that compromises the security or confidentiality of personal information owned or licensed by a person and that causes, reasonably is believed to have caused, or reasonably is believed will cause a material risk of identity theft or other fraud to the person or property of a resident of this state." "['Breach of the security of the system' does not include]: (i) Good faith acquisition of personal information by an employee or agent of the person for the purposes of the person… provided that the personal information is not used for an unlawful purpose or subject to further unauthorized disclosure… [or] (ii) Acquisition of personal information pursuant to a search warrant, subpoena, or other court order,	**Risk of harm threshold exception: Yes** *See Triggering Event* **Encryption exception: Yes** *See Data Regulated* **Hard copy/paper format records in scope: No** *See Triggering Event* **Good faith/agent exception: Yes** *See Triggering Event* **Exception if data was from public records: Yes** *See Data Regulated* **Preempting law: Yes; more restrictive federal or state laws** "A financial institution, trust company, or credit union or any affiliate of a financial institution, trust company, or credit union that is required by federal law, including, but not limited to, any federal statute, regulation, regulatory guidance, or other regulatory action, to notify its customers of an information security breach with respect to information about those customers and that is subject to examination by its functional government regulatory agency for compliance with the applicable federal law, is exempt from the requirements of this [law]." "This [law] does not apply to any person or entity that is a covered

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
	"'Individual' means a natural person." "'Redacted' means altered or truncated so that no more than the last four digits of a social security number, driver's license number, state identification card number, account number, or credit or debit card number is accessible as part of the data."	or pursuant to a subpoena, order, or duty of a regulatory state agency." "'Business entity' means a sole proprietorship, partnership, corporation, association, or other group, however organized and whether operating for profit or not for profit, including a financial institution organized, chartered, or holding a license authorizing operation under the laws of this state, any other state, the United States, or any other country, or the parent or subsidiary of a financial institution." "'Person' has the same meaning as in [Ohio Rev. Code § 1.59, which is an individual, corporation, business trust, estate, trust, partnership, or association], except that 'person' includes a business entity only if the business entity conducts business in this state." "'Record' means any information that is stored in an electronic medium and is retrievable in perceivable form… [but] does not include any publicly available directory containing information an individual voluntarily has consented to have publicly disseminated or listed, such as name, address, or telephone number." "'System' means any collection or group of related records that are kept in an organized manner, that are maintained by a person, and from which personal information is retrieved by the name of the individual or by some identifying number, symbol, or other identifier assigned to the	entity as defined in 45 C.F.R. 160.103, as amended." **Exception recording: No** **Reliance on "no harm" exception requires AG notification: No**

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
		individual… [but] does not include any published directory, any reference material or newsletter, or any routine information that is maintained for the purpose of internal office administration of the person, if the use of the directory, material, newsletter, or information would not adversely affect an individual, and there has been no unauthorized external breach of the directory, material, newsletter, or information."	
Oklahoma Okla. Stat. tit. 24, §§ 161 – 166 (Nov. 1, 2008)	"'Personal information' means the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of this state, when the data elements are neither encrypted nor redacted: a. social security number, b. driver license number or state identification card number issued in lieu of a driver license, or c. financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to the financial accounts of a resident." "['Personal information'] does not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public." "'Encrypted' means transformation of data through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key, or securing the information by	"An individual or entity… [experiences a] breach of the security of the system… [and]encrypted information is accessed and acquired in an unencrypted form or… the security breach involves a person with access to the encryption key and the individual or entity reasonably believes that such breach has caused or will cause identity theft or other fraud to any resident of this state." "An individual or entity that owns or licenses computerized data that includes personal information… discover[s] or [is] notifi[ed] of… [a] breach of the security of the system." "'Breach of the security of a system' means the unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes, or the individual or entity reasonably	**Risk of harm threshold exception: Yes** *See Triggering Event* **Encryption exception: Yes** *See Data Regulated* **Hard copy/paper format records in scope: No** *See Triggering Event* **Good faith/agent exception: Yes** *See Triggering Event* **Exception if data was from public records: Yes** *See Data Regulated* **Preempting law: Yes; more restrictive federal or state laws:** "1. A financial institution that complies with the notification requirements prescribed by the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice

Step 1 - Is Notice Required?
[Back to Introduction]

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
	another method that renders the data elements unreadable or unusable." "'Redact' means alteration or truncation of data such that no more than the following are accessible as part of the personal information: a. five digits of a social security number, or b. the last four digits of a driver license number, state identification card number or account number."	believes has caused or will cause, identity theft or other fraud to any resident of this state." "['Breach of the security of a system' does not include] [g]ood faith acquisition of personal information by an employee or agent of an individual or entity for the purposes of the individual or the entity… provided that the personal information is not used for a purpose other than a lawful purpose of the individual or entity or subject to further unauthorized disclosure." "'Entity' includes corporations, business trusts, estates, partnerships, limited partnerships, limited liability partnerships, limited liability companies, associations, organizations, joint ventures… or any other legal entity, whether for profit or not-for-profit." "'Individual' means a natural person."	is deemed to be in compliance with the provisions of this act. 2. An entity that complies with the notification requirements or procedures pursuant to the rules, regulation, procedures, or guidelines established by the primary or functional federal regulator of the entity shall be deemed to be in compliance with the provisions of this act." **Exception recording: No** **Reliance on "no harm" exception requires AG notification: No**
Oregon Or. Rev. Stat. §§ 646A.600 – 646A.604, 646A.624 – 646A.628 (Jan. 1, 2020)	"'Personal information' means: (A) A consumer's first name or first initial and last name in combination with any one or more of the following data elements, if encryption, redaction or other methods have not rendered the data elements unusable or if the data elements are encrypted and the encryption key has been acquired: (i) A consumer's Social Security number; (ii) A consumer's driver license number or state identification card number issued by the Department of Transportation;	"[A] covered entity is subject to a breach of security or receives notice of a breach of security from a vendor." "A vendor… discovers a breach of security or has reason to believe that a breach of security has occurred." "'Breach of security' means an unauthorized acquisition of computerized data that materially compromises the security, confidentiality or	**Risk of harm threshold exception: Yes** "[A] covered entity 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 covered entity reasonably determines that the consumers whose personal information was

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
	(iii) A consumer's passport number or other identification number issued by the United States; (iv) A consumer's financial account number, credit card number or debit card number, in combination with any required security code, access code or password that would permit access to a consumer's financial account, or any other information or combination of information that a person reasonably knows or should know would permit access to the consumer's financial account; (v) 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; (vi) 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; (vii) Any information about a consumer's medical history or mental or physical condition or about a health care professional's medical diagnosis or treatment of the consumer. (B) A user name or other means of identifying a consumer for the purpose of permitting access to the consumer's account, together with any other method necessary to authenticate the user name or means of identification. (C) Any of the data elements or any combination of the data elements described [in the immediately above two subparagraphs] without the consumer's user name, or the consumer's first name or first initial and last name, if: (i) Encryption, redaction or other methods have not rendered the data element or combination of data elements unusable; and	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." "'Covered entity' means a person 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… [but] does not include [such] a person… to the extent that the person acts solely as a vendor." "'Person' means an individual, private or public corporation, partnership, cooperative, association, estate, limited liability company, organization or other entity, whether or not organized to operate at a profit." "'Vendor' means a person with which a covered entity contracts to maintain, store, manage, process or otherwise access personal information for the purpose of, or in connection with, providing services to or on behalf of the covered entity."	subject to the breach of security are unlikely to suffer harm." **Encryption exception: Yes** *See Data Regulated* **Hard copy/paper format records in scope: No** **Good faith/agent exception: Yes** *See Triggering Event* **Exception if data was from public records: Yes** *See Data Regulated* **Preempting law: Yes;, GLBA, HIPAA, more restrictive federal or state laws** **"**(9) This section does not apply to: (a) Personal information that is subject to, and a person that complies with, notification requirements or procedures for a breach of security that the person's primary or functional federal regulator adopts, promulgates or issues in rules, regulations, procedures, guidelines or guidance, if the personal information and the person would otherwise be subject to ORS 646A.600 to 646A.628. (b) Personal information that is subject to, and a person that complies with, a state or federal law that provides greater protection to personal information and disclosure requirements at

Step 1 - Is Notice Required?
[Back to Introduction]

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
	(ii) The data element or combination of data elements would enable a person to commit identity theft against a consumer." "'Personal information' does not include information in a federal, state or local government record, other than a Social Security number, that is lawfully made available to the public." "'Consumer' means an individual resident of this state." "'Encryption' means an algorithmic process that renders data unreadable or unusable without the use of a confidential process or key." "'Redacted' means altered or truncated so that no more than the last four digits of a Social Security number, driver license number, state identification card number, passport number or other number issued by the United States, financial account number, credit card number or debit card number is visible or accessible."		least as thorough as the protections and disclosure requirements provided under this section. (c) A covered entity or vendor that complies with regulations promulgated under Title V of the Gramm-Leach-Bliley Act of 1999 (15 U.S.C. 6801 to 6809) as that Act existed on January 1, 2020, if personal information that is subject to ORS 646A.600 to 646A.628 is also subject to that Act. (d) A covered entity or vendor that complies with regulations promulgated under the Health Insurance Portability and Accountability Act of 1996 (P.L. 104-191, 110 Stat. 1936) and the Health Information Technology for Economic and Clinical Health Act of 2009 (P.L. 111-5, Title XIII, 123 Stat. 226), as those Acts existed on January 1, 2020, if personal information that is subject to ORS 646A.600 to 646A.628 is also subject to those Acts." **Exception recording: Yes, retain in writing for 5 years** **Reliance on "no harm" exception requires AG notification: No**

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
Pennsylvania 73 Pa. Cons. Stat. §§ 2301 – 2330 (May 2, 2023)	"'Personal information.' (1) An individual's first name or first initial and last name in combination with and linked to any one or more of the following data elements when the data elements are not encrypted or redacted: (i) Social Security number. (ii) Driver's license number or a State identification card number issued in lieu of a driver's license. (iii) Financial account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account. (iv) Medical information. (v) Health insurance information. (vi) A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account." "['Personal information'] does not include publicly available information that is lawfully made available to the general public from Federal, State or local government records or widely distributed media." "'Individual.' [This means] [a] natural person." "'Encryption.' [This means] [t]he use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key." "'Health insurance information.' [This means] [a]n individual's health insurance policy number or subscriber identification number in combination with access code or	"An entity that maintains, stores or manages computerized data that includes personal information shall provide notice of any breach of the security of the system following determination of the breach of the security of the system…" "A vendor that maintains, stores or manages computerized data on behalf of another entity…discover[s] [a breach]." "'Breach of the security of the system.' [This means] [t]he 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 this Commonwealth." "['Breach' includes a security breach in which] encrypted information is accessed and acquired in an unencrypted form… [and] the security breach is linked to a breach of the security of the encryption or… the security breach involves a person with access to the encryption key." "['Breach of the security of the system' does not include] [g]ood faith acquisition of personal information by an employee or agent of the entity for the purposes of the entity… if the personal information is not used for a purpose other than the lawful purpose of the entity and is not subject to further unauthorized disclosure."	**Risk of harm threshold exception: Yes** *See Triggering Event* **Encryption exception: Yes** *See Triggering Event* **Good faith/agent exception: Yes** *See Triggering Event* **Exception if data was from public records: Yes** *See Data Regulated* **Preempting law: Yes; HIPAA, more restrictive federal or state laws** "Any covered entity or business associate that is subject to and in compliance with the privacy and security standards for the protection of electronic personal health information established under the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191, 110 Stat. 1936) and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5, 123 Stat. 226-279 and 467-496) shall be deemed to be in compliance with the provisions of this act." "(a) Information privacy or security policy.--An entity that maintains its own notification procedures as part of an information privacy or security policy for the treatment of

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
	other medical information that permits misuse of an individual's health insurance benefits." "'Medical information.' [This means] [a]ny individually identifiable information contained in the individual's current or historical record of medical history or medical treatment or diagnosis created by a health care professional." "'Redact.' The term includes, but is not limited to, alteration or truncation such that no more than the last four digits of a Social Security number, driver's license number, State identification card number or account number is accessible as part of the data."	"'Business.' [This means] [a] sole proprietorship, partnership, corporation, association or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered or holding a license or authorization certificate under the laws of this Commonwealth, any other state, the United States or any other country, or the parent or the subsidiary of a financial institution… [including] an entity that destroys records." "'Determination.' [This means] [a] verification or reasonable certainty that a breach of the security of the system has occurred." "'Discovery.' [This means] [t]he knowledge of or reasonable suspicion that a breach of the security of the system has occurred." "'Entity.' [This means]… an individual or a business doing business in this Commonwealth." "'Records.' [This means] [a]ny material, regardless of the physical form, on which information is recorded or preserved by any means, including in written or spoken words, graphically depicted, printed or electromagnetically transmitted… [but] does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, such as name, address or telephone number."	personal information and is consistent with the notice requirements of this act shall be deemed to be in compliance with the notification requirements of this act if it notifies subject persons in accordance with its policies in the event of a breach of security of the system. (b) Compliance with Federal requirements.-- (1) A financial institution that complies with the notification requirements prescribed by the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice is deemed to be in compliance with this act. (2) An entity… that complies with the notification requirements or procedures pursuant to the rules, regulations, procedures or guidelines established by the entity's… primary State or functional Federal regulator, shall be in compliance with this act." **Exception recording: No** **Reliance on "no harm" exception requires AG notification: No**

Step 1 - Is Notice Required?
[Back to Introduction]

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
Rhode Island R.I. Gen. Laws § 11-49.3-1, §§ 11-49.3-3 – 11-49.3-6 (Jul. 2, 2016)	"'Personal information' means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or are in hard copy, paper format: (1) Social security number; (2) Driver's license number or Rhode Island identification card number, or tribal identification number; (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. (4) Medical or health insurance information; or (5) Email address with any required security code, access code, or password that would permit access to an individual's personal, medical, insurance, or financial account." "[P]ersonal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records." "'Encrypted' means the transformation of data through the use of a one hundred twenty-eight (128) bit or higher algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key. Data shall not be considered to be encrypted if it is acquired in combination with any key, security code, or password that would permit access to the encrypted data." "'Health insurance information' means an individual's health insurance policy number, subscriber identification	"[A] person that stores, owns, collects, processes, maintains, acquires, uses, or licenses data that includes personal information shall provide notification … of any disclosure of personal information, or any breach of the security system, that poses a significant risk of identity theft to any resident of Rhode Island whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person or entity." "'Breach of the security of the system' means unauthorized access or acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the… person." "['Breach of the security of the system' does not include] [g]ood-faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency… provided, that the personal information is not used or subject to further unauthorized disclosure." "'Owner' means the original collector of the information." "'Person' shall include any individual, sole proprietorship, partnership, association, corporation, joint venture, business, legal entity, trust, estate, cooperative, or other commercial entity."	**Risk of harm threshold exception: Yes** *See Triggering Event* **Encryption exception: Yes** *See Triggering Event* **Hard copy/paper format records in scope: Yes** *See Data Regulated* **Good faith/agent exception: Yes** *See Triggering Event* **Exception if data was from public records: Yes** *See Data Regulated* **Preempting law: Yes; HIPAA, more restrictive federal or state laws** "(a) Any municipal agency, state agency, or person shall be deemed to be in compliance with the security breach notification requirements of § 11-49.3-4 if: (1) The municipal agency, state agency, or person maintains its own security breach procedures as part of an information security policy for the treatment of personal information and otherwise complies with the timing requirements of § 11-49.3-4, and notifies subject persons in accordance with such municipal agency's, state agency's, or person's notification policies in the event of a breach of security; or

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
	number, or any unique identifier used by a health insurer to identify the individual." "'Medical information' means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional or provider."		(2) The person maintains a security breach procedure pursuant to the rules, regulations, procedures, or guidelines established by the primary or functional regulator, as defined in 15 U.S.C. § 6809(2), and notifies subject persons in accordance with the policies or the rules, regulations, procedures, or guidelines established by the primary or functional regulator in the event of a breach of security of the system. (b) A financial institution, trust company, credit union, or its affiliates that is subject to and examined for, and found in compliance with, the Federal Interagency Guidelines on Response Programs for Unauthorized Access to Customer Information and Customer Notice shall be deemed in compliance with this chapter. (c) A provider of health care, healthcare service plan, health insurer, or a covered entity governed by the medical privacy and security rules issued by the federal Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
			and Accountability Act of 1996 (HIPAA) shall be deemed in compliance with this chapter." **Exception recording: No** **Reliance on "no harm" exception requires AG notification: No**
South Carolina S.C. Code § 39-1-90 (Apr. 23, 2013)	"'Personal identifying information' means the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of this State, when the data elements are neither encrypted nor redacted: (a) social security number; (b) driver's license number or state identification card number issued instead of a driver's license; (c) financial account number, or credit card or debit card number in combination with any required security code, access code, or password that would permit access to a resident's financial account; or (d) other numbers or information which may be used to access a person's financial accounts or numbers or information issued by a governmental or regulatory entity that uniquely will identify an individual." "['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."	"A person conducting business in this State, and owning or licensing computerized data or other data that includes personal identifying information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of this State whose personal information was not rendered unusable through encryption, redaction, or other methods was, or is reasonably believed to have been, acquired by an unauthorized person when the illegal use of the information has occurred or is reasonably likely to occur or use of the information creates a material risk of harm to the resident…" "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… discover[s] [a breach]… [and] the personal identifying information was, or is reasonably believed to have been, acquired by an unauthorized person." "'Breach of the security of the system' means unauthorized access to and acquisition of computerized data that was not rendered	**Risk of harm threshold exception: Yes** *See Triggering Event* **Encryption exception: Yes** *See Triggering Event* **Hard copy/paper format records in scope: Yes** *See Triggering Event* **Good faith/agent exception: Yes** *See Triggering Event* **Exception if data was from public records: Yes** *See Data Regulated* **Preempting law: Yes; GLBA, more restrictive federal or state laws** "(I) This section does not apply to a bank or financial institution that is subject to and in compliance with the privacy and security provision of the Gramm-Leach-Bliley Act. (J) A financial institution that is subject to and in compliance with the federal Interagency Guidance Response Programs for Unauthorized Access to Consumer

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
		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." "['Breach of the security of the system' does not include] [g]ood faith acquisition of personal identifying information by an employee or agent of the person for the purposes of its business… if the personal identifying information is not used or subject to further unauthorized disclosure." "'Person' has the same meaning as in [S.C. Code § 37-20-110(10), defined there to mean a natural person, an individual, or a corporation, trust, estate, partnership, cooperative or association]."	Information and Customer Notice, issued March 7, 2005, by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision, as amended, is considered to be in compliance with this section." **Exception recording: No** **Reliance on "no harm" exception requires AG notification: No**
South Dakota S.D. Cod. Laws §§ 22-40-19 – 22-40-26 (Jul. 1, 2018)	"'Personal information,' [meaning] a person's first name or first initial and last name, in combination with any one or more of the following data elements: (a) Social security number; (b) Driver license number or other unique identification number created or collected by a government body; (c) Account, credit card, or debit card number, in combination with any required security code, access code, password, routing number, PIN, or any additional information that would permit access to a person's financial account; (d) Health information as defined in 45 CFR 160.103; or	"Following the discovery by or notification to an information holder of a breach of system security an information holder shall disclose in accordance with § 22-40-22 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." "[D]iscovery by or notification to an information holder of a breach of system security."	**Risk of harm threshold exception: Yes** "…An information holder is not required to make a disclosure … if, following an appropriate investigation and notice to the attorney general, the information holder reasonably determines that the breach will not likely result in harm to the affected person…" **Encryption exception: Yes** *See Data Regulated/Triggering Event*

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
	(e) An identification number assigned to a person by the person's employer in combination with any required security code, access code, password, or biometric data generated from measurements or analysis of human body characteristics for authentication purposes." "['Personal information'] does not include information that is lawfully made available to the general public from federal, state, or local government records or information that has been redacted, or otherwise made unusable." "'Protected information,' includes: (a) A user name or email address, in combination with a password, security question answer, or other information that permits access to an online account; and (b) Account number or credit or debit card number, in combination with any required security code, access code, or password that permits access to a person's financial account."	"'Breach of system security' [means] the unauthorized acquisition of unencrypted computerized data or encrypted computerized data and the encryption key by any person that materially compromises the security, confidentiality, or integrity of personal or protected information maintained by the information holder." "['Breach of system security'] does not include the good faith acquisition of personal or protected information by an employee or agent of the information holder for the purposes of the information holder if the personal or protected information is not used or subject to further unauthorized disclosure." "'Encrypted' [means] computerized data that is rendered unusable, unreadable, or indecipherable without the use of a decryption process or key or in accordance with the Federal Information Processing Standard 140-2 in effect on January 1, 2018." "'Information holder' [means] [a] person or business that conducts business in this state, and that owns or licenses computerized personal or protected information of residents of this state." "'Unauthorized person' [means] any person not authorized to acquire or disclose personal information, or any person authorized by the information holder to access personal information who has acquired or disclosed the personal	**Hard copy/paper format records in scope: No** *See Triggering Event* **Good faith/agent exception: Yes** *See Triggering Event* **Exception if data was from public records: Yes** *See Data Regulated* **Preempting law: Yes; HIPAA, GLBA, more restrictive federal or state laws** "Notwithstanding § 22-40-22, if an information holder maintains its own notification procedure as part of an information security policy for the treatment of personal or protected information and the policy is otherwise consistent with the timing requirements of this section, the information holder is in compliance with the notification requirements of § 22-40-22 if the information holder notifies each person in accordance with the information holder's policies in the event of a breach of system security." "Notwithstanding any other provisions in §§ 22-40-19 to 22-40-26, inclusive, any information holder that is regulated by federal law or regulation, including the Health Insurance Portability and

Step 1 - Is Notice Required?
[Back to Introduction]

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
		information outside the guidelines for access of disclosure established by the information holder."	Accountability Act of 1996 (P.L. 104-191, as amended) or the Gramm Leach Bliley Act (15 U.S.C. § 6801 et seq., as amended) and that maintains procedures for a breach of system security pursuant to the laws, rules, regulations, guidance, or guidelines established by its primary or functional federal regulator is deemed to be in compliance with this chapter if the information holder notifies affected South Dakota residents in accordance with the provisions of the applicable federal law or regulation." **Exception recording: Yes; retain in writing for 3 years** **Reliance on "no harm" exception requires AG notification: Yes** "An information holder is not required to make a disclosure under this section if, following an appropriate investigation and notice to the attorney general, the information holder reasonably determines that the breach will not likely result in harm to the affected person. The information holder shall document the determination under this section in writing and maintain the documentation for not less than three years."

Step 1 - Is Notice Required?
[Back to Introduction]

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
Tennessee Tenn. Code § 47-18-2107 (Apr. 4, 2017)	"'Personal information'… [m]eans an individual's first name or first initial and last name, in combination with any one (1) or more of the following data elements: (i) Social security number; (ii) Driver license number; or (iii) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account." "['Personal information'] [d]oes 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."	"[An information holder] discover[s] or [is] notifi[ed] of a breach of system security." "[An] information holder that maintains computerized data that includes personal information that the information holder does not own… discover[s] or [is] notifi[ed] of [a] breach of system security." "'Breach of system security'… [m]eans the acquisition of the [immediately below] information… by an unauthorized person that materially compromises the security, confidentiality, or integrity of personal information maintained by the information holder: (i) Unencrypted computerized data; or (ii) Encrypted computerized data and the encryption key." "['Breach of system security'] [d]oes not include the good faith acquisition of personal information by an employee or agent of the information holder for the purposes of the information holder if the personal information is not used or subject to further unauthorized disclosure." "'Encrypted' means computerized data that is rendered unusable, unreadable, or indecipherable without the use of a decryption process or key and in accordance with the current version of the Federal Information Processing Standard (FIPS) 140-2."	**Risk of harm threshold exception: No** **Encryption exception: Yes** *See Data Regulated & Triggering Event* **Hard copy/paper format records in scope: No** *See Triggering Event* **Good faith/agent exception: Yes** *See Triggering Event* **Exception if data was from public records: Yes** *See Data Regulated* **Preempting law: Yes; GLBA, more restrictive federal or state laws** "This [law] does not apply to any information holder that is subject to: (1) Title V of the Gramm-Leach-Bliley Act of 1999 (Pub. L. No. 106-102); or (2) [42 U.S.C. §§ 1320d et seq.], as expanded by [42 U.S.C. §§ 300jj et seq. and 42 U.S.C. §§ 17921 et seq.]" "Notwithstanding subsection (e), if an information holder maintains its own notification procedures as part of an information security policy for the treatment of personal information and if the policy is otherwise consistent with the timing requirements of this

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
		"'Information holder' means any person or business that conducts business in this state… that owns or licenses computerized personal information of residents of this state." "'Unauthorized person' includes an employee of the information holder who is discovered by the information holder to have obtained personal information with the intent to use it for an unlawful purpose."	section, the information holder is in compliance with the notification requirements of this section, as long as the information holder notifies subject persons in accordance with its policies in the event of a breach of system security." **Exception recording: No** **Reliance on "no harm" exception requires AG notification: No**
Texas Tex. Bus. & Com. Code § 521.002, § 521.053, § 521.151 **(As amended by SB 768, effective Sep. 1, 2023)**	"'Sensitive personal information' means…: (A) an individual's first name or first initial and last name in combination with any of the following items, if the name and the items are not encrypted: (i) social security number, (ii) driver's license number or government issued identification number, or (iii) account number or credit or debit card number combined with any required security code permitting access to an individual's financial account, or (B) information that identifies an individual and relates to: (i) the physical or mental health or condition of the individual, (ii) the provision of health care to the individual, or (iii) payment for the provision of health care to the individual." "'[S]ensitive personal information' does not include publicly available information that is lawfully made available to the public from the federal government or a state or local government."	"A person who conducts business in this state and owns or licenses computerized data that includes sensitive personal information… discover[s] or receiv[es] notification of [a] breach." "[A] person who maintains computerized data that includes sensitive personal information not owned by the person…discover[s] [a] breach." "'[B]reach of system security' means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt the data." "['Breach of system security' does not include] [g]ood faith acquisition of sensitive personal information by an employee or agent of the person for the purposes of the person… unless the	**Risk of harm threshold exception: No** **Encryption exception: Yes** *See Triggering Event* **Hard copy/paper format records in scope: No** **Good faith/agent exception: Yes** *See Triggering Event* **Exception if data was from public records: Yes** *See Data Regulated* **Preempting law or Policy: No** "Notwithstanding Subsection (e), a person who maintains the person's own notification procedures as part of an information security policy for the treatment of sensitive personal information that complies with the timing requirements for notice under this section complies with this section

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
		person uses or discloses the sensitive personal information in an unauthorized manner."	if the person notifies affected persons in accordance with that policy." **Exception recording: No** **Reliance on "no harm" exception requires AG notification: No**
Utah Utah Code §§ 13-44-101 – 13-44-103, § 13-44-202, § 13-44-301 (May 3, 2023)	"'Personal information' means a person's first name or first initial and last name, combined with any one or more of the following data elements relating to that person when either the name or date [sic] element is unencrypted or not protected by another method that renders the data unreadable or unusable: (i) Social Security number; (ii) (A) financial account number, or credit or debit card number; and (B) any required security code, access code, or password that would permit access to the person's account; or (iii) driver license number or state identification card number." "'Personal information' does not include information regardless of its source, contained in federal, state, or local government records or in widely distributed media that are lawfully made available to the general public."	"A person who owns or licenses computerized data that includes personal information concerning a Utah resident shall, when the person becomes aware of a breach of the system security, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused for identity theft or fraud purposes. If an investigation … reveals that the misuse of personal information for identity theft or fraud purposes has occurred, or is reasonably likely to occur, the person shall provide notification to each affected Utah resident." "A person who maintains computerized data that includes personal information that the person does not own or license…discover[s] [a] breach." "'Breach of system security' means 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	**Risk of harm threshold exception: Yes** *See Triggering Event* **Encryption exception: Yes** *See Data Regulated* **Hard copy/paper format records in scope: No** **Good faith/agent exception: Yes** *See Triggering Event* **Exception if data was from public records: Yes** *See Data Regulated* **Preempting law: Yes; more restrictive federal or state laws** does not apply to a financial institution or an affiliate, as defined in [15 U.S.C. § 6809], of a financial institution." **Risk of Harm Exception: Yes** *See Triggering Event* **Exception recording: No** **Reliance on "no harm" exception requires AG notification: No**

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
		employee or agent of the person possessing unencrypted computerized data… [where] the personal information is [not] used for an unlawful purpose or disclosed in an unauthorized manner."	
Vermont Vt. Stat. tit. 9, § 2430, § 2435 (Jul. 1, 2020)	"'Personally identifiable information' means a consumer's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted or protected by another method that renders them unreadable or unusable by unauthorized persons: (i) a Social Security number; (ii) a driver license or nondriver State identification card number, individual taxpayer identification number, passport number, military identification card number, or other identification number that originates from a government identification document that is commonly used to verify identity for a commercial transaction; (iii) a financial account number or credit or debit card number, if the number could be used without additional identifying information, access codes, or passwords; (iv) a password, personal identification number, or other access code for a financial account; (v) unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee of the data to identify or authenticate the consumer, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data; (vi) genetic information; and	"…[A] data collector that owns or licenses computerized personally identifiable information or login credentials…discover[s] or [is] notifi[ed]… of [a] breach." "[A] data collector that maintains or possesses computerized data containing personally identifiable information or login credentials 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 or login credentials that the data collector does not own or license… discover[s]… [a] breach." "In determining whether personally identifiable information or login credentials have been acquired or is reasonably believed to have been acquired by a person without valid authorization, a data collector may consider the following factors, among others: (i) indications that the information is in the physical possession and control of a person without valid authorization, such as a lost or stolen computer or other device containing information; (ii) indications that the information has been downloaded or copied;	**Risk of harm threshold exception: Yes** "Notice… is not required if the data collector establishes that misuse of personally identifiable information or login credentials is not reasonably possible and the data collector provides notice of the determination that the misuse of the personally identifiable information or login credentials is not reasonably possible pursuant to the requirements of this subsection… If a data collector … subsequently obtains facts indicating that misuse of the personally identifiable information or login credentials has occurred or is occurring, the data collector shall provide notice of the security breach…" **Encryption/Redaction: Yes** *See Data Regulated* **Hard copy/paper format records in scope: Yes, for processors** **Good faith/agent exception: Yes** *See Triggering Event*

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
	(vii)(I) health records or records of a wellness program or similar program of health promotion or disease prevention; (II) a health care professional's medical diagnosis or treatment of the consumer; or (III) a health insurance policy number." "'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." "'Consumer' means an individual residing in this State." "'Encryption' means use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without use of a confidential process or key." "'Login credentials' means a consumer's user name or e-mail address, in combination with a password or an answer to a security question, that together permit access to an online account." "'Redaction' means the rendering of data so that the data are unreadable or are truncated so that no more than the last four digits of the identification number are accessible as part of the data."	(iii) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported; or (iv) that the information has been made public." "'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… private universities, privately and publicly held corporations, limited liability companies, financial institutions, and retail operators." "'Record' means any material on which written, drawn, spoken, visual, or electromagnetic information is recorded or preserved, regardless of physical form or characteristics." "'Security breach' means unauthorized acquisition of electronic data or a reasonable belief of an unauthorized acquisition of electronic data that compromises the security, confidentiality, or integrity of a consumer's personally identifiable information or login credentials maintained by a data collector." "'Security breach' does not include good faith but unauthorized acquisition of personally identifiable information or login credentials by an employee or agent of the data collector for a legitimate purpose of the data collector, provided that the personally identifiable information or login credentials are	**Exception if data was from public records: Yes** *See Data Regulated* **Preempting law: Yes; HIPAA, more restrictive federal or state laws** "A data collector that is subject to the privacy, security, and breach notification rules adopted in 45 C.F.R. Part 164 pursuant to the federal Health Insurance Portability and Accountability Act, P.L. 104-191 (1996) is deemed to be in compliance with this subchapter if: (1) the data collector experiences a security breach that is limited to personally identifiable information specified in 2430(10)(A)(vii); and (2) the data collector provides notice to affected consumers pursuant to the requirements of the breach notification rule in 45 C.F.R. Part 164, Subpart D. (g) Except as provided in subdivision (3) of this subsection, a financial institution that is subject to the following guidances, and any revisions, additions, or substitutions relating to an interagency guidance, shall be exempt from this section:

Step 1 - Is Notice Required?
[Back to Introduction]

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
		not used for a purpose unrelated to the data collector's business or subject to further unauthorized disclosure."	(1) The Federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice, issued on March 7, 2005, by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision. (2) Final Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice, issued on April 14, 2005, by the National Credit Union Administration. (3) A financial institution regulated by the Department of Financial Regulation that is subject to subdivision (1) or (2) of this subsection shall notify the Department as soon as possible after it becomes aware of an incident involving unauthorized access to or use of personally identifiable information. **Exception recording: No Reliance on "no harm" exception requires AG notification: Yes** "If the data collector establishes that misuse of the personally identifiable information or login credentials is not reasonably

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
			possible, the data collector shall provide notice of its determination that misuse of the personally identifiable information or login credentials is not reasonably possible and a detailed explanation for said determination to the Vermont Attorney General or to the Department of Financial Regulation in the event that the data collector is a person or entity licensed or registered with the Department under Title 8 or this title. The data collector may designate its notice and detailed explanation to the Vermont Attorney General or the Department of Financial Regulation as "trade secret" if the notice and detailed explanation meet the definition of trade secret contained in 1 V.S.A. § 317©(9)."
Virginia Va. Code § 18.2-186.6 (Mar. 10, 2020)	"'Personal information' means the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of the Commonwealth, when the data elements are neither encrypted nor redacted: 1. Social security number; 2. Driver's license number or state identification card number issued in lieu of a driver's license number; 3. Financial account number, or credit card or debit card number, in combination with any required security code,	"[A]n individual or entity that owns or licenses computerized data that includes personal information… discover[s] or [is] notifi[ed] of [a] breach of the security of the system." "An individual or entity that maintains computerized data that includes personal information that the individual or entity does not own or license… discover[s]… [a] breach of the security of the system."	**Risk of harm threshold exception: Yes** *See Triggering Event* **Encryption exception: Yes** *See Data Regulated* **Hard copy/paper format records in scope: No** **Good faith/agent exception: Yes** *See Triggering Event*

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
	access code, or password that would permit access to a resident's financial accounts; 4. Passport number; or 5. Military identification number." "['Personal information'] does not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public." "'Encrypted' means the transformation of data through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without the use of a confidential process or key, or the securing of the information by another method that renders the data elements unreadable or unusable." "'Redact' means alteration or truncation of data such that no more than the following are accessible as part of the personal information: 1. Five digits of a social security number; or 2. The last four digits of a driver's license number, state identification card number, or account number."	"'Breach of the security of the system' means the unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes, or the individual or entity reasonably believes has caused, or will cause, identity theft or other fraud to any resident of the Commonwealth." "['Breach' includes breaches in which] [a]n individual or entity['s]… encrypted information is accessed and acquired in an unencrypted form, or… the security breach involves a person with access to the encryption key and the individual or entity reasonably believes that such a breach has caused or will cause identity theft or other fraud to any resident of the Commonwealth." "['Breach of the security of the system' does not include] [g]ood faith acquisition of personal information by an employee or agent of an individual or entity for the purposes of the individual or entity… provided that the personal information is not used for a purpose other than a lawful purpose of the individual or entity or subject to further unauthorized disclosure." "'Entity' includes corporations, business trusts, estates, partnerships, limited partnerships, limited liability partnerships, limited liability companies,	**Exception if data was from public records: Yes** *See Data Regulated* **Preempting law: Yes; HIPAA, more restrictive federal or state laws** "Nothing in this [law] shall apply to an individual or entity regulated by the State Corporation Commission's Bureau of Insurance." "[Provisions regarding a data processor's obligations in relation to breach notification do not apply to a] financial institution or data subject to [15 U.S.C. §§ 6801 et seq.]… [a] covered entity or business associate governed by… 45 C.F.R. Parts 160 and 164 established pursuant to HIPAA, and the Health Information Technology for Economic and Clinical Health Act (P.L. 111-5)… [a] nonprofit organization; or… [an] institution of higher education… [nor do they apply to] information and data [enumerated in Va. Code § 59.1-572(C)(1)–(14)]." **Exception recording: No** **Reliance on "no harm" exception requires AG notification: No**

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
		associations, organizations, joint ventures… or any other legal entity, whether for profit or not for profit." "'Individual' means a natural person."	
Washington Wash. Rev. Code §§ 19.255.005 – 19.255.040 (Mar. 1, 2020)	"'Personal information' means: (i) An individual's first name or first initial and last name in combination with any one or more of the following data elements: (A) Social security number; (B) Driver's license number or Washington identification card number; (C) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account, or any other numbers that can be used to access a person's financial account; (D) Full date of birth; (E) Private key that is unique to an individual and that is used to authenticate or sign an electronic record; (F) Student, military, or passport identification number; (G) Health insurance policy number or health insurance identification number; (H) Any information about a consumer's medical history or mental or physical condition or about a health care professional's medical diagnosis or treatment of the consumer; or (I) Biometric data generated by automatic measurements of an individual's biological characteristics such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual;	"[A] person or business that conducts business in this state and that owns or licenses data that includes personal information shall disclose any breach of the security of the system to any resident of this state whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the personal information was not secured. Notice is not required if the breach of the security of the system is not reasonably likely to subject consumers to a risk of harm. The breach of the secured personal information must be disclosed if the information acquired and accessed is not secured during a security breach or if the confidential process, encryption key, or other means to decipher the secured information was acquired by an unauthorized person." "[A] person or business that maintains or possesses data that may include personal information that the person or business does not own or license… discover[s] [a breach]… [and] the personal information was, or is reasonably believed to have been, acquired by an unauthorized person."	**Risk of harm threshold exception: Yes** *See Triggering Event* **Encryption exception: Yes** *See Data Regulated* **Hard copy/paper format records in scope: Yes** *See Triggering Event* **Good faith/agent exception: Yes** *See Triggering Event* **Exception if data was from public records: Yes** *See Data Regulated* **Preempting law: Yes; HIPAA, more restrictive federal or state laws** "(1) A covered entity under the federal health insurance portability and accountability act of 1996, 42 U.S.C. Sec. 1320d et seq., is deemed to have complied with the requirements of this chapter with respect to protected health information if it has complied with section 13402 of the federal health information

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
	(ii) User name or email address in combination with a password or security questions and answers that would permit access to an online account; and (iii) Any of the data elements or any combination of the data elements described in [Wash. Rev. Code § 19.255.005(2)(a)(i)(A)–(H)]… without the consumer's first name or first initial and last name if: (A) Encryption, redaction, or other methods have not rendered the data element or combination of data elements unusable; and (B) The data element or combination of data elements would enable a person to commit identity theft against a consumer." "Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records."	"'Breach of the security of the system' means unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business." "['Breach of the security of the system' does not include] [g]ood faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business… when the personal information is not used or subject to further unauthorized disclosure." "'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."	technology for economic and clinical health act, P.L. 111-5 as it existed on July 24, 2015. Covered entities shall notify the attorney general pursuant to RCW 19.255.010(7) in compliance with the timeliness of notification requirements of section 13402 of the federal health information technology for economic and clinical health act, P.L. 111-5 as it existed on July 24, 2015, notwithstanding the timeline in RCW 19.255.010(7). (2) A financial institution under the authority of the office of the comptroller of the currency, the federal deposit insurance corporation, the national credit union administration, or the federal reserve system is deemed to have complied with the requirements of this chapter with respect to "sensitive customer information" as defined in the interagency guidelines establishing information 23 security standards, 12 C.F.R. Part 30, Appendix B, 12 C.F.R. Part 24 208, Appendix D-2, 12 C.F.R. Part 225, Appendix F, and 12 C.F.R. Part 25 364, Appendix B, and 12 C.F.R. Part 748, Appendices A and B, as they existed on July 24, 2015, if the financial institution

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
			provides notice to affected consumers pursuant to the interagency guidelines and the notice complies with the customer notice provisions of the interagency guidelines establishing information security standards and the interagency guidance on response programs for unauthorized access to customer information and customer notice under 12 C.F.R. Part 364 as it existed on July 24, 2015. The entity shall notify the 33 attorney general pursuant to RCW 19.255.010 in addition to providing notice to its primary federal regulator." **Exception recording: No** **Reliance on "no harm" exception requires AG notification: No**
West Virginia W. Va. Code §§ 46A-2A-101 – 46A-2A-105 (Jun. 7, 2008)	"'Personal information' means the first name or first initial and last name linked to any one or more of the following data elements that relate to a resident of this state, when the data elements are neither encrypted nor redacted: (A) Social security number; (B) Driver's license number or state identification card number issued in lieu of a driver's license; or (C) Financial account number, or credit card, or debit card number in combination with any required security code,	"An individual or entity that owns or licenses computerized data that includes personal information… discover[s] or [is] notifi[ed] of [a] breach of the security of the system." "An individual or entity that maintains computerized data that includes personal information that the individual or entity does not own or license… discover[s] [a breach]… [and] the personal information was or the entity reasonably	**Risk of harm threshold exception: Yes** *See Triggering Event* **Encryption exception: Yes** *See Data Regulated* **Hard copy/paper format records in scope: No** **Good faith/agent exception: Yes** *See Triggering Event*

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
	access code or password that would permit access to a resident's financial accounts." "['Personal information'] does not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public." "'Encrypted' means transformation of data through the use of an algorithmic process to into a form in which there is a low probability of assigning meaning without use of a confidential process or key or securing the information by another method that renders the data elements unreadable or unusable." "'Redact' means alteration or truncation of data such that no more than the last four digits of a social security number, driver's license number, state identification card number or account number is accessible as part of the personal information."	believes was accessed and acquired by an unauthorized person." "'Breach of the security of a system' means the unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes the individual or entity to reasonably believe that the breach of security has caused or will cause identity theft or other fraud to any resident of this state." "['Breach of the security of a system' includes security breaches in which] encrypted information is accessed and acquired in an unencrypted form… [and security breaches in which the] breach involves a person with access to the encryption key and the individual or entity reasonably believes that such breach has caused or will cause identity theft or other fraud to any resident of this state." "['Breach of the security of a system' does not include] [g]ood faith acquisition of personal information by an employee or agent of an individual or entity for the purposes of the individual or the entity… provided that the personal information is not used for a purpose other than a lawful purpose of the individual or entity or subject to further unauthorized disclosure."	**Exception if data was from public records: Yes** *See Data Regulated* **Preempting law: Yes; more restrictive federal or state laws** "(a) An entity that maintains its own notification procedures as part of an information privacy or security policy for the treatment of personal information and that are consistent with the timing requirements of this article shall be deemed to be in compliance with the notification requirements of this article if it notifies residents of this state in accordance with its procedures in the event of a breach of security of the system. (b) A financial institution that responds in accordance with the notification guidelines prescribed by the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice is deemed to be in compliance with this article. (c) An entity that complies with the notification requirements or procedures pursuant to the rules, regulation, procedures or guidelines established by the entity's primary or functional

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
		"'Entity' includes corporations, business trusts, estates, partnerships, limited partnerships, limited liability partnerships, limited liability companies, associations, organizations, joint ventures… or any other legal entity, whether for profit or not for profit." "'Individual' means a natural person."	regulator shall be in compliance with this article" **Exception recording: No** **Reliance on "no harm" exception requires AG notification: No**
Wisconsin Wis. Stat. §§ 134.98 – 134.99 (Mar. 28, 2008)	"'Personal information' means an individual's last name and the individual's first name or first initial, in combination with and linked to any of the following elements, if the element is not publicly available information and is not encrypted, redacted, or altered in a manner that renders the element unreadable: 1. The individual's social security number. 2. The individual's driver's license number or state identification number. 3. The number of the individual's financial account number, including a credit or debit card account number, or any security code, access code, or password that would permit access to the individual's financial account. 4. The individual's deoxyribonucleic acid profile, as defined in [Wis. Stat. §] 939.74(2d)(a). 5. The individual's unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation." "'Publicly available information' means any information that an entity reasonably believes is one of the following: 1. Lawfully made widely available through any media.	"[A]n entity whose principal place of business is located in this state or an entity that maintains or licenses personal information in this state knows that personal information in the entity's possession has been acquired by a person whom the entity has not authorized to acquire the personal information." "[A]n entity whose principal place of business is not located in this state knows that personal information pertaining to a resident of this state has been acquired by a person whom the entity has not authorized to acquire the personal information." "[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, knows that the personal information has been acquired by a person whom the person storing the personal information has not authorized to acquire the personal information, and the person storing the personal	**Risk of harm threshold exception: Yes** "[A]n entity is not required to provide notice of the acquisition of personal information if any of the following applies:… 1. The acquisition of personal information does not create a material risk of identity theft or fraud to the subject of the personal information…" **Encryption exception: Yes** *See Data Regulated* **Hard copy/paper format records in scope: Yes** *See Triggering Event* **Good faith/agent exception: Yes** "[A]n entity is not required to provide notice of the acquisition of personal information if any of the following applies:… 2. The personal information was acquired in good faith by an employee or

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
	2. 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."	information has not entered into a contract with the person that owns or licenses the personal information." "'Entity' means a person, other than an individual, that does any of the following: a. Conducts business in this state and maintains personal information in the ordinary course of business. b. Licenses personal information in this state. c. Maintains for a resident of this state a depository account as defined in [Wis. Stat. § 815.18(2)€]. d. Lends money to a resident of this state."	agent of the entity, if the personal information is used for a lawful purpose of the entity." **Exception if data was from public records: Yes** *See Data Regulated* **Preempting law: Yes; GLBA, HIPAA** "This [law] does not apply to any of the following: (a) An entity that is subject to, and in compliance with, the privacy and security requirements of [15 U.S.C. §§ 6801 – 6827], or a person that has a contractual obligation to such an entity, if the entity or person has in effect a policy concerning breaches of information security. (b) An entity that is described in 45 CFR 164.104(a), if the entity complies with the requirements of 45 CFR part 164." **Exception recording: No** **Reliance on "no harm" exception requires AG notification: No**
Wyoming Wyo. Stat. §§ 40-12-501 – 40-12-502 (Jul. 1, 2015)	"'Personal identifying information' means the first name or first initial and last name of a person in combination with one (1) or more of the data elements specified in [Wyo. Stat. §] 6-3-901(b)(iii) through (xiv), when the data elements are not redacted."	"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… becomes aware of a breach of the security of the system."	**Risk of harm threshold exception: Yes** *See Triggering Event* **Encryption exception: Redaction** *See Data Regulated*

Step 1 - Is Notice Required?
[Back to Introduction]

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
Wyo. Stat. § 6-3-901(b)(iii)–(xiv) (Jul. 1, 2015)	"[The data elements specified in Wyo. Stat. 6-3-901(b)(iii) through (xiv) are the following, describing an individual person:] (iii) Social security number; (iv) Driver's license number; (v) Account number, credit card number or debit card number in combination with any security code, access code or password that would allow access to a financial account of the person; (vi) Tribal identification card; (vii) Federal or state government issued identification card; (viii) Shared secrets or security tokens that are known to be used for data based authentication;" (ix) A username or email address, in combination with a password or security question and answer that would permit access to an online account; (x) A birth or marriage certificate; (xi) Medical information, meaning a person's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; (xii) Health insurance information, meaning a person's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the person or information related to a person's application and claims history; (xiii) Unique biometric data, meaning data generated from measurements or analysis of human body characteristics for authentication purposes; (xiv) 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	"[A] person who maintains computerized data that includes personal identifying information on behalf of another business entity… determin[es] that personal identifying information was, or is reasonably believed to have been, acquired by an unauthorized person." "'Breach of the security of the data system' means unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal identifying information maintained by a person or business and causes or is reasonably believed to cause loss or injury to a resident of this state." "['Breach of the security of the data system' does not include] [g]ood faith acquisition of personal identifying information by an employee or agent of a person or business for the purposes of the person or business… provided that the personal identifying information is not used or subject to further unauthorized disclosure."	**Hard copy/paper format records in scope: No** **Good faith/agent exception: Yes** *See Triggering Event* **Exception if data was from public records: Yes** *See Data Regulated* **Preempting law: Yes; HIPAA:** "A covered entity or business associate that is subject to and complies with the Health Insurance Portability and Accountability Act, and the regulations promulgated under that act, 45 C.F.R. Parts 160 and 164, is deemed to be in compliance with this section if the covered entity or business associate notifies affected Wyoming customers or entities in compliance with the requirements of the Health Insurance Portability and Accountability Act and 45 C.F.R. Parts 160 and 164." **Exception recording: No** **Reliance on "no harm" exception requires AG notification: No**

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
	distributed media that are lawfully made available to the general public." "'Redact' means alteration or truncation of data such that no more than five (5) digits of the data elements provided [as forms of personal identifying information] are accessible as part of the personal information."		
District of Columbia D.C. Code §§ 28-3851 – 28-3853 (Jun. 17, 2020)	"'Personal information' means: (i) An individual's first name, first initial and last name, or any other personal identifier, which, in combination with any of the following data elements, can be used to identify a person or the person's information: (I) Social security number, Individual Taxpayer Identification Number, passport number, driver's license number, District of Columbia identification card number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual; (II) Account number, credit card number or debit card number, or any other number or code or combination of numbers or codes, such as an identification number, security code, access code, or password, that allows access to or use of an individual's financial or credit account; (III) Medical information; (IV) Genetic information and deoxyribonucleic acid profile; (V) Health insurance information, including a policy number, subscriber information number, or any unique identifier used by a health insurer to identify the person that permits access to an individual's health and billing information;	"[A] 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… discovers a breach of the security of the system." "[A] 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… discover[s] [a security breach]." "'Breach of the security of the system' means unauthorized acquisition of computerized or other electronic data, or any equipment or device storing such data, that compromises the security, confidentiality, or integrity of personal information maintained by the person or entity who conducts business in the District of Columbia." "The term 'breach of the security system' does not include: (i) A good-faith acquisition of personal information by an employee or agent of the person or entity	**Risk of harm threshold exception: Yes** *See Triggering Event* **Encryption exception: Yes** *See Triggering Event* **Hard copy/paper format records in scope: No** **Good faith/agent exception: Yes** *See Triggering Event* **Exception if data was from public records: Yes** *See Data Regulated* **Preempting law: Yes; GLBA, HIPAA** "A person or entity that maintains procedures for a breach notification system under Title V of the Gramm-Leach-Bliley Act, approved November 12, 1999 (113 Stat. 1436; 15 U.S.C. § 6801 et seq.), or the breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
	(VI) Biometric data of an individual generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voice print, genetic print, retina or iris image, or other unique biological characteristic, that is used to uniquely authenticate the individual's identity when the individual accesses a system or account; or (VII) Any combination of data elements included [above] that would enable a person to commit identity theft without reference to a person's first name or first initial and last name or other independent personal identifier. (ii) A user name or e-mail address in combination with a password, security question and answer, or other means of authentication, or any combination of data elements included in [the immediately above sub-sub-subparagraph] that permits access to an individual's e-mail account." "The term 'personal information' shall not include publicly available information that is lawfully made available to the general public from federal, state, or local government records." "'Genetic information' has the meaning ascribed to it under the federal Health Insurance Portability and Accountability Act of 1996." "'Medical Information' means any information about a consumer's dental, medical, or mental health treatment or diagnosis by a health-care professional."	for the purposes of the person or entity if the personal information is not used improperly or subject to further unauthorized disclosure; (ii) 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; or (iii) Acquisition of personal information of an individual that the person or entity reasonably determines, after a reasonable investigation and consultation with the Office of the Attorney General for the District of Columbia and federal law enforcement agencies, will likely not result in harm to the individual." "'Person or entity' means an individual, firm, corporation, partnership, company, cooperative, association, trust, or any other organization, legal entity, or group of individuals."	Regulations, established pursuant to the Health Insurance Portability Accountability Act of 1996, approved August 21, 1996 (Pub. L. No. 104-191; 110 Stat. 1936), or the Health Information Technology for Economic and Clinical Health Act, approved February 17, 2009 (Pub. L. No. 111-5; 123 Stat. 226), and provides notice in accordance with such Acts, and any rules, regulations, guidance and guidelines thereto, to each affected resident in the event of a breach, shall be deemed to be in compliance with this section with respect to the notification of residents whose personal information is included in the breach. The person or entity shall, in all cases, provide written notice of the breach of the security of the system to the Office of the Attorney General for the District of Columbia as required under subsection (b-1) of this section." **Exception recording: No** **Reliance on "no harm" exception requires AG notification: Yes** *See Triggering Event*
Guam	"Personal information means the first name, or first initial, and last name in combination with and linked to any one	"An individual or entity that owns or licenses computerized data that includes personal	**Risk of harm threshold exception: Yes**

Step 1 - Is Notice Required?
[Back to Introduction]

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
9 Guam Code §§ 48.20 – 48.50 (Jul. 11, 2009)	or more of the following data elements that relate to a resident of Guam, when the data elements are neither encrypted nor redacted: (1) Social Security number; (2) Driver's license number or Guam identification card number issued in lieu of a driver's license; or (3) Financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial accounts." "[Personal information] does not include information that is lawfully obtained from publicly available information, or from Federal, State, or local government records lawfully made available to the general public." "Encrypted means transformation of data through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without the use of a confidential process or key, or securing the information by another method that renders the data elements unreadable or unusable." "Redact means alteration or truncation of data such that no more than the following are accessible as part of the personal information: (1) five (5) digits of a Social Security Number, or (2) The last four (4) digits of a driver's license number, Guam identification card number or financial account number."	information… discover[s] or [is] notifi[ed] of [a] breach of the security of the system." "An individual or entity that maintains computerized data that includes personal information that the individual or entity does not own or license… discover[s] [a security breach]." "Breach of the security of a system means the unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes, or the individual or entity reasonably believes has caused or will cause, identity theft or other fraud to any resident of Guam." "[Breach of the security of the system includes breaches in which] encrypted information is accessed and acquired in an unencrypted form… [and breaches where] the security breach involves a person with access to the encryption key and the individual or entity reasonably believes that such breach has caused or will cause identity theft or other fraud to any resident of Guam." "[Breach of the security of a system does not include] [g]ood faith acquisition of personal information by an employee or agent of an individual or entity for the purposes of the individual or the entity… provided, that the personal information is not used for a purpose	*See Triggering Event* **Encryption exception: Yes** *See Triggering Event* **Hard copy/paper format records in scope: No** **Good faith/agent exception: Yes** *See Triggering Event* **Exception if data was from public records: Yes** *See Data Regulated* **Preempting law: No** "This Chapter deals with subject matter that is of island-wide concern, and it is the intent of *I Liheslatura* that this Chapter shall supersede and preempt all rules and regulations during the matters expressly set forth in this Chapter." **Exception recording: No** **Reliance on "no harm" exception requires AG notification: No**

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
		other than a lawful purpose of the individual or entity or subject to further unauthorized disclosure." "Entity includes corporations, business trusts, estates, partnerships, limited partnerships, limited liability partnerships, limited liability companies, associations, organizations, joint ventures… or any other legal entity, whether for profit or not-for-profit." "Individual means a natural person."	
Puerto Rico P.R. Laws tit. 10, §§ 4051 – 4055 (Jun. 19, 2008)	"Personal information file… [means] a file containing at least the name or first initial and the surname of a person, together with any of the following data so that an association may be established between certain information with another and in which the information is legible enough so that in order to access it there is no need to use a special cryptographic code. (1) Social security number. (2) Driver's license number, voter's identification or other official identification. (3) Bank or financial account numbers of any type with or without passwords or access code that may have been assigned. (4) Names of users and passwords or access codes to public or private information systems. (5) Medical information protected by the HIPAA. (6) Tax information. (7) Work-related evaluations."	"[An] entity that is the owner or custodian of a database that includes personal information of citizens residents of Puerto Rico… [experiences a breach, and] the database whose security has been breached contains, in whole or in part, personal information files and the same are not protected by an encrypted code but only by a password." "Entity… [m]eans every… corporation, partnership, association, private company or organization authorized to do business or operate in the Commonwealth of Puerto Rico; as well as every… private educational institution, regardless of the level of education offered by it." "Violation of the security system… [m]eans 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,	**Risk of harm threshold exception: No** **Encryption exception: Yes** *See Data Regulated, Triggering Event* **Hard copy/paper format records in scope: Arguably no** *See Triggering Event* **Good faith/agent exception: Yes** **Exception if data was from public records: Yes** *See Data Regulated* **Preempting law: No** **Exception recording: No** **Reliance on "no harm" exception requires AG notification: No**

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
	"[Personal information file does not include] the mailing nor the residential address… [n]or information that is a public document and that is available to the citizens in general."	confidentiality or integrity of the information in the data bank has been compromised; or when normally authorized persons or entities have had access and it is known or there is reasonable suspicion that they have violated the professional confidentiality or obtained authorization under false representation with the intention of making illegal use of the information. This includes both access to the data banks through the system and physical access to the recording media that contain the same and any removal or undue retrieval of said recordings."	
Virgin Islands V.I. Code tit. 14, § 2200, §§ 2209 – 2211 (Oct. 17, 2005)	"'[P]ersonal information' means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social Security number. (2) Driver's license number. (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account." "'[P]ersonal information' does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records."	"[A] person or business that conducts business in the Virgin Islands, and that owns or licenses computerized data that includes personal information… discover[s] or [is] notifi[ed] of [a] breach in the security of the data." "[A] person or business that maintains computerized data that includes personal information that the person or business does not own… discover[s] [a breach]." "'[B]reach of the security of the system' means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business." "['Breach of the security of the system' does not include] [g]ood faith acquisition of personal information by an employee or agent of the	**Risk of harm threshold exception: No** **Encryption exception: Yes** *See Data Regulated* **Hard copy/paper format records in scope: No** *See Triggering Event* **Good faith/agent exception: Yes** *See Triggering Event* **Exception if data was from public records: Yes** *See Data Regulated* **Preempting law: No** **Exception recording: No** **Reliance on "no harm" exception requires AG notification: No**

Step 1 - Is Notice Required?
[Back to Introduction]

State & Statute	Data Regulated	Triggering Event	Exceptions/Other Criteria
		person or business for the purposes of the person or business… provided that the personal information is not used or subject to further unauthorized disclosure."	

Step 2 – How and When to Notify Individuals?

[Back to Introduction]

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
Alabama Ala. Code §§ 8-38-1 – 8-38-9, 8-38-11 – 8-38-12 (Jun. 1, 2018)	"A covered entity that is not a third-party agent… shall give notice… to each individual." "[A] third-party agent [that] has experienced a breach of security in the system maintained by the 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. After receiving notice from a third-party agent, a covered entity shall provide [the] notices required." "Notice to individuals… shall be made as expeditiously as possible and without unreasonable delay, taking into account the time necessary to allow the covered entity to conduct an investigation in accordance with [Ala. Code §] 8-38-4. "[T]he covered entity shall provide notice within 45 days of the covered entity's receipt of notice from a third-party agent that a breach has occurred or upon the covered entity's determination that a breach has occurred and is reasonably likely to cause substantial harm to the individuals to whom the information relates… [but] [i]f a federal or state law enforcement agency determines that notice to individuals… 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. A law enforcement agency, by a subsequent written request, may revoke the	"The notice shall include, at a minimum, all of the following: (1) The date, estimated date, or estimated date range of the breach. (2) A description of the sensitive personally identifying information that was acquired by an unauthorized person as part of the breach. (3) A general description of the actions taken by a covered entity to restore the security and confidentiality of the personal information involved in the breach. (4) A general description of steps an affected individual can take to protect himself or herself from identity theft. (5) Information that the individual can use to contact the covered entity to inquire about the breach."

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	delay as of a specified date or extend the period set forth in the original request… if further delay is necessary." "[N]otice to an affected individual… shall be given in writing, sent to the mailing address of the individual in the records of the covered entity, or by email notice sent to the email address of the individual in the records of the covered entity… [but] [a] covered entity required to provide notice to any individual… may provide substitute notice in lieu of direct notice, if direct notice is not feasible due to any of the following: a. Excessive cost. The term includes either of the following: 1. Excessive cost to the covered entity relative to the resources of the covered entity. 2. The cost to the covered entity exceeds five hundred thousand dollars ($500,000). b. Lack of sufficient contact information for the individual required to be notified. c. The affected individuals exceed 100,000 persons. Substitute notice shall include both of the following: 1. A conspicuous notice on the Internet website of the covered entity, if the covered entity maintains a website, for a period of 30 days. 2. Notice in print and in broadcast media, including major media in urban and rural areas where the affected individuals reside. b. An alternative form of substitute notice may be used with the approval of the Attorney General."	
Alaska Alaska Stat. §§ 45.48.010 – 45.48.090	"[T]he covered person shall… disclose the breach to each state resident whose personal information was subject to the breach."	*(Not provided for.)*

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
(Jul. 1, 2009)	"An information collector shall make the disclosure required… in the most expeditious time possible and without unreasonable delay, except as… necessary to determine the scope of the breach and restore the reasonable integrity of the information system… [and except that] [a]n information collector may delay disclosing the breach… if an appropriate law enforcement agency determines that disclosing the breach will interfere with a criminal investigation. However, the information collector shall disclose the breach to the state resident in the most expeditious time possible and without unreasonable delay after the law enforcement agency informs the information collector in writing that disclosure of the breach will no longer interfere with the investigation." "If an information recipient notifies an information distributor of a [a breach of the security of the information system containing personal information on a state resident that is maintained by an information recipient]… the information distributor shall comply with [notice obligations] as if the breach occurred to the information system maintained by the information distributor." "An information collector shall make the disclosure required… (1) by a written document sent to the most recent address the information collector has for the state resident; (2) by electronic means if the information collector's primary method of communication with the state resident is by electronic means or if making the disclosure by the electronic means is consistent with [15 U.S.C. §§ 7001 et seq.]…; or (3) if the information collector demonstrates that the cost of providing notice would exceed $150,000, that the	

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	affected class of state residents to be notified exceeds 300,000, or that the information collector does not have sufficient contact information to provide notice, by (A) electronic mail if the information collector has an electronic mail address for the state resident; (B) conspicuously posting the disclosure on the Internet website of the information collector if the information collector maintains an Internet website; and (C) providing a notice to major statewide media." "[I]mmediately after the information recipient discovers [a breach of the security of the information system containing personal information on a state resident that is maintained by an information recipient], the information recipient shall notify the information distributor who owns the personal information or who licensed the use of the personal information to the information recipient about the breach." "'[I]nformation distributor' means a person who is an information collector and who owns or licenses personal information to an information recipient." "'[I]nformation 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."	
Arizona Ariz. Rev. Stat. § 18-551, § 18-552	"[T]he person that owns or licenses the [breached] computerized data, within forty-five days after the determination [of the breach], shall… [n]otify the individuals affected… [but notification] may be delayed if a	"The notification required… shall include at least the following: 1. The approximate date of the breach. 2. A brief description of the personal information included in the breach.

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
(Aug. 3, 2018; as amended Mar 29, 2022)	law enforcement agency advises the person that the notifications will impede a criminal investigation. On being informed by the law enforcement agency that the notifications no longer compromise the investigation, the person shall make the required notifications, as applicable, within forty-five days." "'Individual' means a resident of this state who has a principal mailing address in this state as reflected in the records of the person conducting business in this state at the time of the breach." "A 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." "The notification required… shall be provided by one of the following methods: 1. Written notice. 2. An e-mail notice if the person has e-mail addresses for the individuals who are subject to the notice. 3. Telephonic notice, if telephonic contact is made directly with the affected individuals and is not through a prerecorded message. 4. Substitute notice if the person demonstrates that the cost of providing notice pursuant to [the immediately above] paragraph[s] 1, 2 or 3… would exceed fifty thousand dollars, that the affected class of subject individuals to be notified exceeds one hundred thousand individuals, or that the person does not have sufficient contact information. Substitute notice consists of all of the following: (a) A written letter to the attorney general that demonstrates the facts necessary for substitute notice.	3. The toll-free numbers and addresses for the three largest nationwide consumer reporting agencies. 4. The toll-free number, address, and website address for the federal trade commission or any federal agency that assists consumers with identity theft matters." "'Nationwide consumer reporting agency': (a) Means a consumer reporting agency that compiles and maintains files on consumers on a nationwide basis as defined in [15 U.S.C. § 1681a(p)]. (b) Does not include a nationwide specialty consumer reporting agency as defined in [15 U.S.C. § 1681a(x)]."

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	(b) Conspicuous posting of the notice for at least forty-five days on the website of the person if the person maintains one." "If a breach involves personal information [that is an individual's user name or e-mail address, in combination with a password or security question and answer, that allows access to an online account] for an online account and does not involve personal information [that is the individual's first name or first initial and last name in combination with one or more data elements specified in Ariz. Rev. Stat. § 18-551(11)] the person may… provid[e] the notification in an electronic or other form that directs the individual whose personal information has been breached to promptly change the individual's password and security question or answer, as applicable, or to take other steps that are appropriate to protect the online account with the person and all other online accounts for which the individual whose personal information has been breached uses the same user name and e-mail address and password or security question or answer. If the breach of personal information [that is that is an individual's user name or e-mail address, in combination with a password or security question and answer, that allows access to an online account] is for login credentials of an e-mail account furnished by the person, the person is not required to… provid[e] the notification to that e-mail address, but may… provid[e] notification [with regard to the individual's account with the person] by another method described in [Ariz. Rev. Stat. § 18-552(G)] or by providing clear and conspicuous notification delivered to the individual online when the individual is connected to the online account from an internet protocol address or online location from which the person knows the individual customarily	

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	accesses the account… [or by] requiring the individual to reset the individual's password or security question and answer for that account, if the person also notifies the individual to change the same password or security question and answer for all other online accounts for which the individual uses the same user name or e-mail address and password or security question or answer."	
Arkansas Ark. Code §§ 4-110-101 – 4-110-108 (Jul. 23, 2019)	"[A] person or business that acquires, owns, or licenses computerized data that includes personal information shall disclose any breach… to any resident of Arkansas whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." "The disclosure shall be made in the most expedient time and manner possible and without unreasonable delay, consistent with… any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system… [but] [t]he [individual] notification… may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation… [in which case] [t]he notification… shall be made after the law enforcement agency determines that it will not compromise the investigation." "A person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner of licensee." "[N]otice may be provided by one (1) of the following methods: (1) Written notice;	*(Not provided for.)*

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	(2) Electronic mail notice if the notice provided is consistent with [15 U.S.C. § 7001], as it existed on January 1, 2005; or (3) (A) Substitute notice if the person or business demonstrates that: (i) The cost of providing notice would exceed two hundred fifty thousand dollars ($250,000); (ii) The affected class of persons to be notified exceeds five hundred thousand (500,000); or (iii) The person or business does not have sufficient contact information. (B) Substitute notice shall consist of all of the following: (i) Electronic mail notice when the person or business has an electronic mail address for the subject persons; (ii) Conspicuous posting of the notice on the website of the person or business if the person or business maintains a website; and (iii) Notification by statewide media."	
California Cal. Civ. Code § 1798.80, § 1798.82, § 1798.84, § 1798.150 (Jan. 1, 2021; § 1798.150 eff. Jan. 1, 2023)	"A person or business that conducts business California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system… to a[n] [affected] resident of California." "A person or business that maintains the computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of the breach of the security of the data." "The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement… or any measures necessary to determine the scope of the breach and	"The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the [required] information… under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice." "The format of the notice shall be designed to call attention to the nature and significance of the information it contains… [t]he title and headings in the notice shall be clearly and conspicuously displayed… [and] [t]he text of the notice and any other notice… shall be no smaller than 10-point type." "The security breach notification… shall include, at a minimum, the following information: (A) The name and contact information of the reporting person or business.

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	restore the reasonable integrity of the data system… [but] [t]he notification… may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification… shall be made promptly after the law enforcement agency determines that it will not compromise the investigation." "'[N]otice' may be provided by one of the following methods: (1) Written notice. (2) Electronic notice, if the notice provided is consistent with [15 U.S.C. § 7001]. (3) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following: (A) Email notice when the person or business has an email address for the subject persons. (B) Conspicuous posting, for a minimum of 30 days, of the notice on the internet website page of the person or business, if the person or business maintains one… [Here,] conspicuous posting on the person's or business' internet website means providing a link to the notice on the home page or first significant page after entering the internet website that is in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks that call attention to the link. (C) Notification to major statewide media."	(B) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach. (C) If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice. (D) Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided. (E) A general description of the breach incident, if that information is possible to determine at the time the notice is provided. (F) The toll-free telephone numbers and addresses of the major credit reporting agencies, if the breach exposed a social security number or a driver's license or California identification card number." "At the discretion of the person or business, the security breach notification may also include any of the following: (A) Information about what the person or business has done to protect individuals whose information has been breached. (B) Advice on steps that people whose information has been breached may take to protect themselves. (C) In breaches involving biometric data, instructions on how to notify other entities that used the same type of biometric data as an authenticator to no longer rely on data for authentication purposes." "If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information [that is a Social Security number, driver's license number, California identification card number, Tax Identification Number, or other unique government identifier]."

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	"In the case of a breach of the security of the system involving personal information [that is a username or email address, in combination with a password or security question and answer that would permit access to an online account] for an online account, and no other personal information defined in [Cal. Civ. Code § 1798.82(h)(1)], the person or business may… provid[e] the security breach notification in electronic or other form that directs the person whose personal information has been breached promptly to change the person's password and security question or answer, as applicable, or to take other steps appropriate to protect the online account with the person or business and all other online accounts for which the person whose personal information has been breached uses the same username or email address and password or security question or answer." "In the case of a breach of the security of the system involving personal information [that is a username or email address, in combination with a password or security question and answer that would permit access to an online account] for login credentials of an email account furnished by the person or business, the person or business shall not… provid[e] the security breach notification to that email address, but may, instead… provid[e] notice by another method described in [Cal. Civ. Code § 1798.82(j)] or by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an Internet Protocol address or online location from which the person or business knows the resident customarily accesses the account."	

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
Colorado Colo. Rev. Stat. § 6-1-716 (Sep. 1, 2018)	"[A] covered entity shall give notice to the affected Colorado residents… in the most expedient time possible and without unreasonable delay, but not later than thirty days after the date of determination that a security breach occurred, consistent with… any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system… [but individual] notice… may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation and the law enforcement agency has notified the covered entity that conducts business in Colorado not to send [individual] notice… [In that case,] [n]otice… must be made in good faith, in the most expedient time possible and without unreasonable delay, but not later than thirty days after the law enforcement agency determines that notification will no longer impede the investigation and has notified the covered entity that conducts business in Colorado that it is appropriate to send the notice." "If a covered entity uses a third-party service provider to maintain computerized data that includes personal information, then the third-party service provider shall… [notify] the covered entity of any security breach in the most expedient time possible, and without unreasonable delay." "'Notice' means: (I) Written notice to the postal address listed in the records of the covered entity; (II) Telephonic notice; (III) Electronic notice, if a primary means of communication by the covered entity with a Colorado resident is by	"[N]otice required… to affected Colorado residents must include, but need not be limited to, the following information: (I) The date, estimated date, or estimated date range of the security breach; (II) A description of the personal information that was acquired or reasonably believed to have been acquired as part of the security breach; (III) Information that the resident can use to contact the covered entity to inquire about the security breach; (IV) The toll-free numbers, addresses, and websites for consumer reporting agencies; (V) The toll-free number, address, and website for the federal trade commission; and (VI) A statement that the resident can obtain information from the federal trade commission and the credit reporting agencies about fraud alerts and security freezes."

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	electronic means or the notice provided is consistent with [15 U.S.C. §§ 7001 et seq.]; or (IV) Substitute notice, if the covered entity required to provide notice demonstrates that the cost of providing notice will exceed two hundred fifty thousand dollars, the affected class of persons to be notified exceeds two hundred fifty thousand Colorado residents, or the covered entity does not have sufficient contact information to provide notice. Substitute notice consists of all of the following: (A) E-mail notice if the covered entity has e-mail addresses for the members of the affected class of Colorado residents; (B) Conspicuous posting of the notice on the website page of the covered entity if the covered entity maintains one; and (C) Notification to major statewide media." "If… the covered entity… determines that the [personal information that is a Colorado resident's username or e-mail address, in combination with a password or security questions and answers, that would permit access to an online account] has been misused or is reasonably likely to be misused, then the covered entity shall [additionally]: (I) Direct the person whose personal information has been breached to promptly change his or her password and security question or answer, as applicable, or to take other steps appropriate to protect the online account with the covered entity and all other online accounts for which the person whose personal information has been breached uses the same username or e-mail address and password or security question or answer. (II) For log-in credentials of an e-mail account furnished by the covered entity, the covered entity shall not… provid[e]	

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	the security breach notification to that e-mail address, but may instead… provid[e] notice through other methods, as defined in [Colo. Rev. Stat. § 6-1-716(1)(f)], or by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an internet protocol address or online location from which the covered entity knows the resident customarily accesses the account." "'Determination that a security breach occurred' means the point in time at which there is sufficient evidence to conclude that a security breach has taken place."	
Connecticut Conn. Gen. Stat. § 36a-701b as amended by P.A. 21-59 (Oct. 1, 2021)	"[A] person who owns, licenses or maintains computerized data that includes personal information, shall provide notice of any breach of security… to any resident of this state whose personal information was breached or is reasonably believed to have been breached. Such notice shall be made without unreasonable delay but not later than sixty days after the discovery of such breach, unless a shorter time is required under federal law…If the person identifies additional residents of this state whose personal information was breached or reasonably believed to have been breached following sixty days after the discovery of such breach, the person shall proceed in good faith to notify such additional residents as expediently as possible… [but] [a]ny [individual] notification… shall be delayed for a reasonable period of time if a law enforcement agency determines that the notification will impede a criminal investigation and such law enforcement agency has made a request that the notification be delayed. Any such delayed notification shall be made after such law enforcement agency determines that notification will not compromise	"[In breaches involving] a breach of login credentials [that are a user name or electronic mail address, in combination with a password or security question and answer that would permit access to an online account]… notice to a resident [should]… direct[] the resident whose personal information was breached or is reasonably believed to have been breached to promptly change any password or security question and answer, as applicable, or to take other appropriate steps to protect the affected online account and all other online accounts for which the resident uses the same user name or electronic mail address and password or security question and answer." "The person who owns or licenses computerized data that includes personal information, shall offer to each resident whose… [Social Security number or taxpayer identification number] was breached or is reasonably believed to have been breached, appropriate identity theft prevention services and, if applicable, identity theft mitigation services. Such service or services shall be provided at no cost to such resident for a period of not less than twenty-four months. Such person shall provide all information necessary for such resident to enroll in such service or services and shall include information on how such resident can place a credit freeze on such resident's credit file."

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	the criminal investigation and so notifies the person of such determination." "[A] person that maintains computerized data that includes personal information that the person does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following its discovery." "[A] notice… may be provided by one of the following methods [by default]: (1) Written notice; (2) telephone notice; (3) electronic notice, provided such notice is consistent with [15 U.S.C. § 7001]; (4) substitute notice, provided such person demonstrates that the cost of providing notice in accordance with [the immediately above] subdivision[s] (1), (2) or (3)… would exceed two hundred fifty thousand dollars, that the affected class of subject persons to be notified exceeds five hundred thousand persons or that the person does not have sufficient contact information." "Substitute notice shall consist of the following: (A) Electronic mail notice when the person has an electronic mail address for the affected persons; (B) conspicuous posting of the notice on the web site of the person if the person maintains one; and (C) notification to major state-wide media, including newspapers, radio and television." "[But in breaches involving] a breach of login credentials [that are a user name or electronic mail address, in combination with a password or security question and answer that would permit access to an online account]…	

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	notice to a resident may be provided in electronic or other form that [contains prescribed content]." "[Further, where the breached person] furnishes an electronic mail account… [they may not] provid[e] notification to the electronic mail account that was breached or reasonably believed to have been breached if the person cannot reasonably verify the affected resident's receipt of such notification… [and instead they] shall provide notice by another method described in this section or by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an Internet protocol address or online location from which the person knows the resident customarily accesses the account."	
Delaware Del. Code tit. 6 §§ 12B-101 – 12B-104 (Apr. 14, 2018)	"A[] person who conducts business in this State and who owns or licenses computerized data that includes personal information shall provide notice of any breach of security… to any resident of this State whose personal information was breached or is reasonably believed to have been breached." "A person that maintains computerized data that includes personal information that the person does not own or license shall give notice to… the owner or licensee of the information of any breach of security immediately following determination of the breach of security." "Notice [to individuals]… must be made without unreasonable delay but not later than 60 days after determination of the breach of security… [unless] [a] shorter time is required under federal law… [or] [a] law-	"If the breach of security includes a Social Security number, the person shall offer to each resident, whose personal information, including Social Security number, was breached or is reasonably believed to have been breached, credit monitoring services at no cost to such resident for a period of 1 year. Such person shall provide all information necessary for such resident to enroll in such services and shall include information on how such resident can place a credit freeze on such resident's credit file. Such services are not required if, after an appropriate investigation, the person reasonably determines that the breach of security is unlikely to result in harm to the individuals whose personal information has been breached."

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	enforcement agency determines that the notice will impede a criminal investigation and such law-enforcement agency has made a request of the person that the notice be delayed. Any such delayed notice must be made after such law-enforcement agency determines that notice will not compromise the criminal investigation and so notifies the person of such determination." "When a person otherwise required… to provide [individual] notice, could not, through reasonable diligence, identify within 60 days that the personal information of certain residents of this State was included in a breach of security, such person must provide the [individual] notice… to such residents as soon as practicable after the determination that the breach of security included the personal information of such residents, unless such person provides or has provided substitute notice." "Notice' means any of the following: a. Written notice. b. Telephonic notice. c. Electronic notice, if the notice provided is consistent with [15 U.S.C. § 7001] or if the person's primary means of communication with the resident is by electronic means. d. Substitute notice, if the person required to provide notice… demonstrates that the cost of providing notice will exceed $75,000, or that the affected number of Delaware residents to be notified exceeds 100,000 residents, or that the person does not have sufficient contact information to provide notice. Substitute notice consists of all of the following: 1. Electronic notice if the person has email addresses for the members of the affected class of Delaware residents.	

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	2. Conspicuous posting of the notice on a website page of the person if the person maintains 1 or more website pages. 3. Notice to major statewide media, including newspapers, radio, and television and publication on the major social media platforms of the person providing notice." "In the case of a breach of security involving personal information [that is a username or email address, in combination with a password or security question and answer that would permit access to an online account] for login credentials of an email account furnished by the person, the person cannot… provid[e] the security breach notification to such email address, but may instead… provid[e] notice by another method described in [Del. Code tit. 6, § 12B-101(5)] or by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an Internet Protocol address or online location from which the person knows the resident customarily accesses the account."	
Florida Fla. Stat. § 501.171 (Oct. 1, 2019)	"A covered entity shall give notice to each individual in this state whose personal information was, or the covered entity reasonably believes to have been, accessed as a result of the breach. Notice to individuals shall be made as expeditiously as practicable and without unreasonable delay, taking into account the time necessary to allow the covered entity to determine the scope of the breach of security, to identify individuals affected by the breach, and to restore the reasonable integrity of the data system that was breached, but no later than 30 days after the determination of a breach or reason to believe a breach occurred unless… a federal, state, or local law enforcement	"The notice to an individual with respect to a breach of security shall include, at a minimum: 1. The date, estimated date, or estimated date range of the breach of security. 2. A description of the personal information that was accessed or reasonably believed to have been accessed as a part of the breach of security. 3. Information that the individual can use to contact the covered entity to inquire about the breach of security and the personal information that the covered entity maintained about the individual."

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	agency determines that notice to individuals… would interfere with a criminal investigation, [in which case] the notice shall be delayed upon the written request of the law enforcement agency for a specified period that the law enforcement agency determines is reasonably necessary. A law enforcement agency may, by a subsequent written request, revoke such delay as of a specified date or extend the period set forth in the original request… to a specified date if further delay is necessary." "In the event of a breach of security of a system maintained by a third-party agent, such third-party agent shall notify the covered entity of the breach of security as expeditiously as practicable, but no later than 10 days following the determination of the breach of security or reason to believe the breach occurred. Upon receiving notice from a third-party agent, a covered entity shall provide notices required [to individuals]." "The notice to an affected individual shall be by one of the following methods: 1. Written notice sent to the mailing address of the individual in the records of the covered entity; or 2. E-mail notice sent to the e-mail address of the individual in the records of the covered entity." "A covered entity required to provide notice to an individual may provide substitute notice in lieu of direct notice if such direct notice is not feasible because the cost of providing notice would exceed $250,000, because the affected individuals exceed 500,000 persons, or because the covered entity does not have an e-mail address or mailing address for the affected individuals. Such substitute notice shall include the following:	

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	1. A conspicuous notice on the Internet website of the covered entity if the covered entity maintains a website; and 2. Notice in print and to broadcast media, including major media in urban and rural areas where the affected individuals reside."	
Georgia Ga. Code § 10-1-911, § 10-1-912 (May 24, 2007)	"[An] information broker… that maintains computerized data that includes personal information of individuals shall give notice of any breach of the security of the system… to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The notice shall be made in the most expedient time possible and without unreasonable delay, consistent with… any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system… [but notice] may be delayed if a law enforcement agency determines that the notification will compromise a criminal investigation. The notification… shall be made after the law enforcement agency determines that it will not compromise the investigation." "[A] person or business that maintains computerized data on behalf of an information broker… that includes personal information of individuals that the person or business does not own shall notify the information broker… of any breach of the security of the system within 24 hours following discovery." "'Notice' means: (A) Written notice;	*(Not provided for.)*

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	(B) Telephone notice; (C) Electronic notice, if the notice provided is consistent with [15 U.S.C. § 7001]; or (D) Substitute notice, if the information broker… demonstrates that the cost of providing notice would exceed $50,000.00, that the affected class of individuals to be notified exceeds 100,000, or that the information broker… does not have sufficient contact information to provide written or electronic notice to such individuals. Substitute notice shall consist of all of the following: (i) E-mail notice, if the information broker… has an e-mail address for the individuals to be notified; (ii) Conspicuous posting of the notice on the information broker's… website page, if the information broker… maintains one; and (iii) Notification to major state-wide media."	
Hawai'i Haw. Rev. Code §§ 487N-1 – 487N-3 (Jul. 1, 2008)	"[A] business that owns or licenses personal information of residents of Hawai'i, [or] [a] business that conducts business in Hawai'i that owns or licenses personal information in any form (whether computerized, paper, or otherwise)… shall provide notice to the affected person that there has been a security breach… The disclosure notification shall be made without unreasonable delay, consistent with the legitimate needs of law enforcement… and consistent with any measures necessary to determine sufficient contact information, determine the scope of the breach, and restore the reasonable integrity, security, and confidentiality of the data system." "[A] business located in Hawai'i or [a] business that conducts business in Hawai'i that maintains or possesses records or data containing personal information of	"The notice shall be clear and conspicuous… [and] shall include a description of the following: (1) The incident in general terms; (2) The type of personal information that was subject to the unauthorized access and acquisition; (3) The general acts of the business… to protect the personal information from further unauthorized access; (4) A telephone number that the person may call for further information and assistance, if one exists; and (5) Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports."

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	residents of Hawai'i that the business does not own or license… shall notify the owner or licensee of the information of any security breach immediately following discovery of the breach, consistent with the legitimate needs of law enforcement." "[The legitimate needs of law enforcement means that notice] shall be delayed if a law enforcement agency informs the business… that notification may impede a criminal investigation or jeopardize national security and requests a delay; provided that such request is made in writing, or the business… documents the request contemporaneously in writing, including the name of the law enforcement officer making the request and the officer's law enforcement agency engaged in the investigation. The notice… shall be provided without unreasonable delay after the law enforcement agency communicates to the business… its determination that notice will no longer impede the investigation or jeopardize national security." "[N]otice to affected persons may be provided by one of the following methods: (1) Written notice to the last available address the business… has on record; (2) Electronic mail notice, for those persons for whom a business… has a valid electronic mail address and who have agreed to receive communications electronically if the notice provided is consistent with [15 U.S.C. § 7001]; (3) Telephonic notice, provided that contact is made directly with the affected persons; and (4) Substitute notice, if the business… demonstrates that the cost of providing notice would exceed $100,000 or that the affected class of subject persons to be notified exceeds	

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	two hundred thousand, or if the business… does not have sufficient contact information or consent to satisfy [the immediately above] paragraph[s] (1), (2), or (3), for only those affected persons without sufficient contact information or consent, or if the business… is unable to identify particular affected persons, for only those unidentifiable affected persons. Substitute notice shall consist of all the following: (A) Electronic mail notice when the business… has an electronic mail address for the subject persons; (B) Conspicuous posting of the notice on the website page of the business… if one is maintained; and (C) Notification to major statewide media."	
Idaho Idaho Code §§ 28-51-104 – 28-51-107 (Jul. 1, 2015)	"[An] 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… shall give notice as soon as possible to the affected Idaho resident. Notice must be made in the most expedient time possible and without unreasonable delay, consistent with… any measures necessary to determine the scope of the breach, to identify the individuals affected, and to restore the reasonable integrity of the computerized data system… [but notice] may be delayed if a law enforcement agency advises the… individual or commercial entity that the notice will impede a criminal investigation. Notice… must be made in good faith, without unreasonable delay and as soon as possible after the law enforcement agency advises the… individual or commercial entity that notification will no longer impede the investigation." "[An] individual or a commercial entity that maintains computerized data that includes personal information that	*(Not provided for.)*

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	the… individual or the commercial entity does not own or license shall give notice to… the owner or licensee of the information of any breach of the security of the system immediately following discovery of a breach." "'Notice' means: (a) Written notice to the most recent address the… individual or commercial entity has in its records; (b) Telephonic notice; (c) Electronic notice, if the notice provided is consistent with [15 U.S.C. § 7001]; or (d) Substitute notice, if the… individual or the commercial entity required to provide notice demonstrates that the cost of providing notice will exceed twenty-five thousand dollars ($25,000), or that the number of Idaho residents to be notified exceeds fifty thousand (50,000), or that the… individual or the commercial entity does not have sufficient contact information to provide notice. Substitute notice consists of all of the following: (i) E-mail notice if the… individual or the commercial entity has e-mail addresses for the affected Idaho residents; and (ii) Conspicuous posting of the notice on the website page of the… individual or the commercial entity if the… individual or the commercial entity maintains one; and (iii) Notice to major statewide media."	
Illinois 815 Ill. Comp. Stat. §§ 530/1 – 530/10, §§ 530/15 –	"[A] data collector that owns or licenses personal information concerning an Illinois resident shall notify the resident at no charge that there has been a breach of the security of the system data… The disclosure notification shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and	"The disclosure notification to an Illinois resident shall include, but need not be limited to, information as follows: (1) With respect to personal information [that is an individual's first name or first and initial and last name in combination with at least one data element listed in 815 Ill. Comp. Stat. 530/5(1)]: (A) the toll-free numbers and addresses for consumer reporting agencies;

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
530/20 (Jan. 1, 2020)	restore the reasonable integrity, security, and confidentiality of the data system… [but notice] may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the data collector with a written request for the delay. However, the data collector must notify the Illinois resident as soon as notification will no longer interfere with the investigation." "[A] 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 shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery." "[N]otice to consumers may be provided by one of the following methods: (1) written notice; (2) electronic notice, if the notice provided is consistent with [15 U.S.C. § 7001]; or (3) substitute notice, if the data collector demonstrates that the cost of providing notice would exceed $250,000 or that the affected class of subject persons to be notified exceeds 500,000, or the data collector does not have sufficient contact information. Substitute notice shall consist of all of the following: (i) email notice if the data collector has an email address for the subject persons; (ii) conspicuous posting of the notice on the data collector's web site page if the data collector maintains one; and (iii) notification to major statewide media or, if the breach impacts residents in one geographic area, to prominent local media in areas where affected individuals are likely to	(B) the toll-free number, address, and website address for the Federal Trade Commission; and (C) a statement that the individual can obtain information from these sources about fraud alerts and security freezes. (2) With respect to personal information [that is a user name or email address, in combination with a password or security question and answer that would permit access to an online account], notice may… [direct] the Illinois resident whose personal information has been breached to promptly change his or her user name or password and security question or answer, as applicable, or to take other steps appropriate to protect all online accounts for which the resident uses the same user name or email address and password or security question and answer." "The [individual] notification shall not… include information concerning the number of Illinois residents affected by the breach."

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	reside if such notice is reasonably calculated to give actual notice to persons whom notice is required."	
Indiana Ind. Code §§ 24-4.9-1 – 24-4.9-5 (Jul. 1, 2017, as amended Mar. 18, 2022)	"[T]he data base owner shall disclose the breach to an Indiana resident whose: (1) unencrypted personal information was or may have been acquired by an unauthorized person; or (2) encrypted personal information was or may have been acquired by an unauthorized person with access to the encryption key." "A person that maintains computerized data but that is not a data base owner shall notify the data base owner." "A person required to make a disclosure or notification… shall make the disclosure or notification without unreasonable delay, but not more than forty-five (45) days after the discovery of the breach… [A] delay is reasonable if the delay is: (1) necessary to restore the integrity of the computer system; (2) necessary to discover the scope of the breach; or (3) in response to a request from the attorney general or a law enforcement agency to delay disclosure because disclosure will: (A) impede a criminal or civil investigation; or (B) jeopardize national security." "A person required to make a disclosure or notification… shall make the disclosure or notification as soon as possible after:	*(Not provided for.)*

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	(1) delay is no longer necessary to restore the integrity of the computer system or to discover the scope of the breach; or (2) the attorney general or a law enforcement agency notifies the person that delay will no longer impede a criminal or civil investigation or jeopardize national security." "[A] data base owner required to make a disclosure… shall make the disclosure using one (1) of the following methods: (1) Mail. (2) Telephone. (3) Facsimile (fax). (4) Electronic mail, if the data base owner has the electronic mail address of the affected Indiana resident." "If a data base owner required to make a disclosure… is required to make the disclosure to more than five hundred thousand (500,000) Indiana residents, or if the data base owner required to make a disclosure… determines that the cost of the disclosure will be more than two hundred fifty thousand dollars ($250,000), the data base owner required to make a disclosure… may elect to make the disclosure by using both of the following methods: (1) Conspicuous posting of the notice on the web site of the data base owner, if the data base owner maintains a web site. (2) Notice to major news reporting media in the geographic area where Indiana residents affected by the breach of the security of a system reside."	

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
Iowa Iowa Code §§ 715C.1 – 715C.2 (Jul. 1, 2018)	"[A] person who owns or licenses computerized data that includes a consumer's personal information that is used in the course of the person's business, vocation, occupation, or volunteer activities and that was subject to a breach of security shall give notice of the breach of security… to any consumer whose personal information was included in the information that was breached." "'Consumer' means an individual who is a resident of this state." "The consumer notification shall be made in the most expeditious manner possible and without unreasonable delay, consistent with… any measures necessary to sufficiently determine contact information for the affected consumers, determine the scope of the breach, and restore the reasonable integrity, security, and confidentiality of the data… [but notice] may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation and the agency has made a written request that the notification be delayed. The notification… shall be made after the law enforcement agency determines that the notification will not compromise the investigation and notifies the person required to give notice in writing." "[A] person who maintains or otherwise possesses personal information on behalf of another person shall notify the owner or licensor of the information of any breach of security immediately following discovery of such breach of security." "[N]otification to the consumer may be provided by one of the following methods:	"Notice… shall include, at a minimum, all of the following: a. A description of the breach of security. b. The approximate date of the breach of security. c. The type of personal information obtained as a result of the breach of security. d. Contact information for consumer reporting agencies. e. Advice to the consumer to report suspected incidents of identity theft to local law enforcement or the attorney general." "'Consumer reporting agency' means the same as defined by [15 U.S.C. § 1681a]."

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	a. Written notice to the last available address the person has in the person's records. b. Electronic notice if the person's customary method of communication with the consumer is by electronic means or is consistent with [Iowa Code §§ 554D et seq.] and [15 U.S.C. § 7001]. c. Substitute notice, if the person demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars, that the affected class of consumers to be notified exceeds three hundred fifty thousand persons, or if the person does not have sufficient contact information to provide notice. Substitute notice shall consist of the following: (1) Electronic mail notice when the person has an electronic mail address for the affected consumers. (2) Conspicuous posting of the notice or a link to the notice on the internet website of the person if the person maintains an internet website. (3) Notification to major statewide media."	
Kansas Kan. Stat. §§ 50-7a01 – 50-7a02 (Jul. 1, 2006)	"A person that conducts business in this state… that owns or licenses computerized data that includes personal information shall… give notice… to the affected Kansas residents. Notice must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system." "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	*(Not provided for.)*

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	license shall give notice to the owner or licensee of the information of any breach of the security of the data following discovery of a breach." "Notice… may be delayed if a law enforcement agency determines that notice will impede a criminal investigation. [In that case] [n]otice… shall be made in good faith, without unreasonable delay and as soon as possible after the law enforcement agency determines that notification will no longer impede the investigation." "'Notice' means: (1) Written notice; (2) electronic notice, if the notice provided is consistent with [15 U.S.C. § 7001]; or (3) substitute notice, if the individual or the commercial entity required to provide notice demonstrates that the cost of providing notice will exceed $100,000, or that the affected class of consumers to be notified exceeds 5,000, or that the individual or the commercial entity does not have sufficient contact information to provide notice." "'Substitute notice' means: (1) E-mail notice if the individual or the commercial entity has e-mail addresses for the affected class of consumers; (2) conspicuous posting of the notice on the web site page of the individual or the commercial entity if the individual or the commercial entity maintains a web site; and (3) notification to major statewide media."	
Kentucky Ky. Rev. Stat. § 365.732	"[An] information holder shall disclose any breach of the security of the system… to any resident of Kentucky whose unencrypted personal information was, or is reasonably	*(Not provided for.)*

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
(Jul. 15, 2014)	believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement… or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system." "[An] information holder that maintains computerized data that includes personally identifiable information that the information holder does not own shall notify the owner or licensee of the information of any breach of the security of the data as soon as reasonably practicable following discovery." "[N]otification… may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification… shall be made promptly after the law enforcement agency determines that it will not compromise the investigation." "[N]otice may be provided by one (1) of the following methods: (a) Written notice; (b) Electronic notice, if the notice provided is consistent with [15 U.S.C. § 7001]; or (c) Substitute notice, if the information holder demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds five hundred thousand (500,000), or the information holder does not have sufficient contact information. Substitute notice shall consist of all of the following:	

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	1. E-mail notice, when the information holder has an e-mail address for the subject persons; 2. Conspicuous posting of the notice on the information holder's Internet Web site page, if the information holder maintains a Web site page; and 3. Notification to major statewide media."	
Louisiana La. Rev. Stat. §§ 51:3071 – 51:3077 (Aug. 1, 2018) La. Admin. Code tit. 16, pt. III, § 701 (Mar. 20, 2007)	"[A] person that owns or licenses computerized data that includes personal information… shall… notify any resident of the state whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person." "[A] person that maintains computerized data that includes personal information that the… person does not own shall notify the owner or licensee of the [breach]… following discovery by the… person of [the] breach of security of the system." "The notification… shall be made in the most expedient time possible and without unreasonable delay but not later than sixty days from the discovery of the breach, consistent with… any measures necessary to determine the scope of the breach, prevent further disclosures, and restore the reasonable integrity of the data system… [but] [i]f a law enforcement agency determines that the notification… would impede a criminal investigation, such notification may be delayed until such law enforcement agency determines that the notification will no longer compromise such investigation." "[In the case that] notification [to individuals or to the information owner or licensee]… is [lawfully] delayed… the	*(Not provided for.)*

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	person… shall provide the attorney general the reasons for the delay in writing within the sixty day [individual] notification period… Upon receipt of the written reasons, the attorney general shall allow a reasonable extension of time to provide the notification." "Notification may be provided by one of the following methods: (1) Written notification. (2) Electronic notification, if the notification provided is consistent with [15 U.S.C. § 7001]. (3) Substitute notification, if…[a] person demonstrates that the cost of providing notification would exceed one hundred thousand dollars, or that the affected class of persons to be notified exceeds one hundred thousand, or the… person does not have sufficient contact information. Substitute notification shall consist of all of the following: (a) E-mail notification when the agency or person has an e-mail address for the subject persons. (b) Conspicuous posting of the notification on the Internet site of the agency or person, if an Internet site is maintained. (c) Notification to major statewide media."	
Maine Me. Stat. tit. 10, §§ 1346 – 1350-A (Sep. 19, 2019)	"[A]n information broker that maintains computerized data that includes personal information… shall give notice of a breach of the security of the system… to a resident of this State whose personal information has been, or is reasonably believed to have been, acquired by an unauthorized person." "[A]ny other person who maintains computerized data that includes personal information… shall give notice of a	*(Not provided for.)*

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	breach of the security of the system… to a resident of this State if misuse of the personal information has occurred or if it is reasonably possible that misuse will occur." "A 3rd-party entity that maintains, on behalf of a person, computerized data that includes personal information that the 3rd-party entity does not own shall notify the person maintaining personal information of a breach of the security of the system immediately following discovery." "[N[otice]… must be made as expediently as possible and without unreasonable delay, consistent with… measures necessary to determine the scope of the security breach and restore the reasonable integrity, security and confidentiality of the data in the system… [and] must be made no more than 30 days after the person… becomes aware of a breach of security and identifies its scope… [but notice] 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." "'Notice' means: A. Written notice; B. Electronic notice, if the notice provided is consistent with [15 U.S.C. § 7001]; or C. Substitute notice, if the person maintaining personal information demonstrates that the cost of providing notice would exceed $5,000, that the affected class of individuals to be notified exceeds 1,000 or that the person maintaining personal information does not have sufficient contact information to provide written or electronic notice to those individuals. Substitute notice must consist of all of the following:	

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	(1) E-mail notice, if the person has e-mail addresses for the individuals to be notified; (2) Conspicuous posting of the notice on the person's publicly accessible website, if the person maintains one; and (3) Notification to major statewide media."	
Maryland Md. Com. Law §§ 14-3501 – 14-3508 (Oct. 1, 2022)	"[T]he owner or licensee of the [breached] computerized data shall notify the [affected] individual of the breach… as soon as reasonably practicable, but not later than 45 days after the business discovers or is notified of the breach of the security of a system." "A business that maintains computerized data that includes personal information of an individual residing in the State that the business does not own or license… shall notify, as soon as practicable, the owner or licensee of the personal information of the breach of the security of a system… as soon as reasonably practicable, but not later than 10 days after the business discovers or is notified of the breach of the security of a system." "[N]otification… may be delayed: (i) If a law enforcement agency determines that the notification will impede a criminal investigation or jeopardize homeland or national security; or (ii) To determine the scope of the breach of the security of a system, identify the individuals affected, or restore the integrity of the system." "If notification is delayed [by such a law enforcement agency determination]… notification shall be given as soon as reasonably practicable, but not later than:	"[If the breach involves personal information other than only personal information that permits access to an individual's e-mail account,] [t]he notification… shall include: (1) To the extent possible, a description of the categories of information that were, or are reasonably believed to have been, acquired by an unauthorized person, including which of the elements of personal information were, or are reasonably believed to have been, acquired; (2) Contact information for the business making the notification, including the business' address, telephone number, and toll-free telephone number if one is maintained; (3) The toll-free telephone numbers and addresses for the major consumer reporting agencies; and (4) (i) The toll-free telephone numbers, addresses, and website addresses for: 1. The Federal Trade Commission; and 2. The Office of the Attorney General; and (ii) A statement that an individual can obtain information from these sources about steps the individual can take to avoid identity theft."

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	(I) For a notification required [by a business that owns, licenses, or maintains the breached data]: 1. 7 days after the law enforcement agency determines that it will not impede a criminal investigation and will not jeopardize homeland or national security if the original 45-day period has already elapsed; or 2. The end of the original 45-day period; or (II) For a notification required [by a business that maintains the breached data that the business does not own or license], 7 days after the law enforcement agency determines that it will not impede a criminal investigation and will not jeopardize homeland or national security" "[N]otification… shall be given: (1) By written notice sent to the most recent address of the individual in the records of the business; (2) By electronic mail to the most recent electronic mail address of the individual in the records of the business, if: (i) The individual has expressly consented to receive electronic notice; or (ii) The business conducts its business primarily through Internet account transactions or the Internet; (3) By telephonic notice, to the most recent telephone number of the individual in the records of the business; or (4) By substitute notice… if the business does not have sufficient contact information to give notice in accordance with [the immediately above] item[s] (1), (2), or (3)." "Substitute notice… shall consist of: (1) Electronically mailing the notice to an individual entitled to notification… if the business has an electronic mail address for the individual to be notified; (2) Conspicuous posting of the notice on the website of the business, if the business maintains a website; and	

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	(3) Notification to major print or broadcast media in geographic areas where the individuals affected by the breach likely reside." "In the case of a breach of the security of a system involving personal information that permits access to an individual's e–mail account [as defined in Md. Com. Law § 14–3501(e)(1)(ii)] and no other personal information [as defined in Md. Com. Law § 14–3501(e)(1)(i)], the business may… provid[e] the notification in electronic or other form that directs the individual whose personal information has been breached promptly to: (i) Change the individual's password and security question or answer, as applicable; or (ii) Take other steps appropriate to protect the e-mail account with the business and all other online accounts for which the individual uses the same user name or e-mail and password or security question or answer." "[In this case] the notification… may not be given to the individual by sending notification by e-mail to the e-mail account affected by the breach… [and] may be given by a clear and conspicuous notice delivered to the individual online while the individual is connected to the affected e-mail account from an Internet Protocol address or online location from which the business knows the individual customarily accesses the account."	
Massachusetts Mass. Gen. Laws §§ 93H-1 – 93H-6 (Apr. 10, 2019)	"A person… that owns or licenses data that includes personal information about a resident of the commonwealth, shall provide notice, as soon as practicable and without unreasonable delay… to such resident."	"[N]otice… shall include, but shall not be limited to: (i) the resident's right to obtain a police report; (ii) how a resident may request a security freeze and the necessary information to be provided when requesting the security freeze; (iii) that there shall be no charge for a security freeze; and

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	"A person… that maintains or stores, but does not own or license data that includes personal information about a resident of the commonwealth, shall provide notice, as soon as practicable and without unreasonable delay… to the owner or licensor." "[N]otice may be delayed if a law enforcement agency determines that provision of such notice may impede a criminal investigation and has notified the attorney general, in writing, thereof and informs the person… of such determination. If notice is delayed due to such determination and as soon as the law enforcement agency determines and informs the person… that notification no longer poses a risk of impeding an investigation, notice shall be provided, as soon as practicable and without unreasonable delay." ''Notice'' shall include:— (i) written notice; (ii) electronic notice, if notice provided is consistent with [15 U.S.C. § 7001(c)]; and [Mass. Gen. Laws §§ 110G et seq.]; or (iii) substitute notice, if the person… demonstrates that the cost of providing written notice will exceed $250,000, or that the affected class of Massachusetts residents to be notified exceeds 500,000 residents, or that the person… does not have sufficient contact information to provide notice." ''Substitute notice'', shall consist of all of the following:— (i) electronic mail notice, if the person… has electronic mail addresses for the members of the affected class of Massachusetts residents;	(iv) mitigation services to be provided pursuant to this [law]; provided, however, that said notice shall not include the nature of the breach of security or unauthorized acquisition or use, or the number of residents of the commonwealth affected by said breach of security or unauthorized access or use." "If the person… that experienced a breach of security is owned by another person or corporation, the notice… shall include the name of the parent or affiliated corporation." "If a person knows or has reason to know that said person experienced an incident that requires notice pursuant to section 3 and such breach of security includes a social security number, the person shall contract with a third party to offer to each resident whose social security number was disclosed in the breach of security or is reasonably believed to have been disclosed in the breach of security, credit monitoring services at no cost to said resident for a period of not less than 18 months..."

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	(ii) clear and conspicuous posting of the notice on the home page of the person… if the person… maintains a website; and (iii) publication in or broadcast through media or medium that provides notice throughout the commonwealth."	
Michigan Mich. Comp. Laws §§ 445.61 – 445.64, § 445.72, § 445.72b (Jan. 1, 2020)	"[A] person… that owns or licenses data that are included in a database… shall provide a notice of the security breach to each resident of this state who meets 1 or more of the following: (a) That resident's unencrypted and unredacted personal information was accessed and acquired by an unauthorized person. (b) That resident's personal information was accessed and acquired in encrypted form by a person with unauthorized access to the encryption key." "[A] person… that maintains a database that includes data that the person or agency does not own or license… shall provide a notice to the owner or licensor of the information of the security breach." "A person… shall provide any [individual] notice… without unreasonable delay… [but] may delay providing notice… if either of the following is met: (a) A delay is necessary in order for the person… to take any measures necessary to determine the scope of the security breach and restore the reasonable integrity of the database. However, the… person shall provide the notice… without unreasonable delay after the person or agency completes the measures necessary to determine the scope of the security breach and restore the reasonable integrity of the database.	"[Notice] shall do all of the following: (a) For [electronic or written notice]… be written in a clear and conspicuous manner and contain the content required under [the immediately below] subdivisions (c) to (g). (b) For [telephonic notice]… clearly communicate the content required under [the immediately below] subdivisions (c) to (g) to the recipient of the telephone call. (c) Describe the security breach in general terms. (d) Describe the type of personal information that is the subject of the unauthorized access or use. (e) If applicable, generally describe what the… person providing the notice has done to protect data from further security breaches. (f) Include a telephone number where a notice recipient may obtain assistance or additional information. (g) Remind notice recipients of the need to remain vigilant for incidents of fraud and identity theft." "[Substitute notice via notification to major statewide media] shall include a telephone number or a website address that a person may use to obtain additional assistance and information."

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	(b) A law enforcement agency determines and advises the… person that providing a notice will impede a criminal or civil investigation or jeopardize homeland or national security. However, the… person shall provide the notice… without unreasonable delay after the law enforcement agency determines that providing the notice will no longer impede the investigation or jeopardize homeland or national security." "[A] person shall provide any notice… by providing 1 or more of the following to the recipient: (a) Written notice sent to the recipient at the recipient's postal address in the records of the… person. (b) Written notice sent electronically to the recipient if any of the following are met: (i) The recipient has expressly consented to receive electronic notice. (ii) The person… has an existing business relationship with the recipient that includes periodic electronic mail communications and based on those communications the person… reasonably believes that it has the recipient's current electronic mail address. (iii) The person… conducts its business primarily through internet account transactions or on the internet. (c) If not otherwise prohibited by state or federal law, notice given by telephone by an individual who represents the person… if all of the following are met: (i) The notice is not given in whole or in part by use of a recorded message. (ii) The recipient has expressly consented to receive notice by telephone, or if the recipient has not expressly consented to receive notice by telephone, the person… also provides notice under [the immediately above] subdivision[s] (a) or (b) if the notice by telephone does not	

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	result in a live conversation between the individual representing the person… and the recipient within 3 business days after the initial attempt to provide telephonic notice. (d) Substitute notice, if the person… demonstrates that the cost of providing notice under [the immediately above] subdivision[s] (a), (b), or (c) will exceed $250,000.00 or that the person… has to provide notice to more than 500,000 residents of this state. A person… provides substitute notice… by doing all of the following: (i) If the person… has electronic mail addresses for any of the residents of this state who are entitled to receive the notice, providing electronic notice to those residents. (ii) If the person… maintains a website, conspicuously posting the notice on that website. (iii) Notifying major statewide media."	
Minnesota Minn. Stat. § 325E.61 (Jul. 1, 2006)	"[A] person or business that conducts business in this state, and that owns or licenses data that includes personal information, shall disclose any breach of the security of the system… to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with… any measures necessary to determine the scope of the breach, identify the individuals affected, and restore the reasonable integrity of the data system… [but notice] may be delayed to a date certain if a law enforcement agency affirmatively determines that the notification will impede a criminal investigation."	*(Not provided for.)*

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	"[A] person or business that maintains data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery." "'[N]otice' may be provided by one of the following methods: (1) written notice to the most recent available address the person or business has in its records; (2) electronic notice, if the person's primary method of communication with the individual is by electronic means, or if the notice provided is consistent with [15 U.S.C. § 7001]; or (3) substitute notice, if the person or business demonstrates that the cost of providing notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. Substitute notice must consist of all of the following: (i) e-mail notice when the person or business has an e-mail address for the subject persons; (ii) conspicuous posting of the notice on the Web site page of the person or business, if the person or business maintains one; and (iii) notification to major statewide media."	
Mississippi Miss. Code § 75-24-29 (Jul. 1, 2021)	"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, subject to… the completion of an investigation by the person to determine the nature and scope of the incident, to identify the affected individuals, or to restore the	*(Not provided for.)*

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	reasonable integrity of the data system… [but notice] shall be delayed for a reasonable period of time if a law enforcement agency determines that the notification will impede a criminal investigation or national security and the law enforcement agency has made a request that the notification be delayed. Any such delayed notification shall be made after the law enforcement agency determines that notification will not compromise the criminal investigation or national security and so notifies the person of that determination." "'Affected individual' means [an] individual who is a resident of this state whose personal information was, or is reasonably believed to have been, intentionally acquired by an unauthorized person through a breach of security." "[A] person who conducts business in this state that maintains computerized data which includes personal information that the person does not own or license shall notify the owner or licensee of the information of any breach of the security of the data as soon as practicable following its discovery." "[N]otice… may be provided by one (1) of the following methods: (a) written notice; (b) telephone notice; (c) electronic notice, if the person's primary means of communication with the affected individuals is by electronic means or if the notice is consistent with [15 U.S.C. § 7001]; or (d) substitute notice, provided the person demonstrates that the cost of providing notice in accordance with [the immediately above] paragraph[s] (a), (b) or (c)… would exceed Five Thousand Dollars ($	

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	5,000.00), that the affected class of subject persons to be notified exceeds five thousand (5,000) individuals or the person does not have sufficient contact information. Substitute notice shall consist of the following: electronic mail notice when the person has an electronic mail address for the affected individuals; conspicuous posting of the notice on the Web site of the person if the person maintains one; and notification to major statewide media, including newspapers, radio and television."	
Missouri Mo. Rev. Stat. § 407.1500 (Aug. 28, 2009)	"[A] 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 shall provide notice to the affected consumer that there has been a breach of security… The disclosure notification shall be: (a) Made without unreasonable delay; (b) Consistent with the legitimate needs of law enforcement…; and (c) Consistent with any measures necessary to determine sufficient contact information and to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system." "[A] 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 information of a resident of Missouri that the person does not own or license, shall notify the owner or license of the information of any breach of security immediately following discovery of the	"The notice shall at minimum include a description of the following: (a) The incident in general terms; (b) The type of personal information that was obtained as a result of the breach of security; (c) A telephone number that the affected consumer may call for further information and assistance, if one exists; (d) Contact information for consumer reporting agencies; (e) Advice that directs the affected consumer to remain vigilant by reviewing account statements and monitoring free credit reports." "'Consumer reporting agency' [has] the same as defined by [15 U.S.C. § 1681a]."

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	breach, consistent with the legitimate needs of law enforcement." "[Consistent with the legitimate needs of law enforcement means that] [n]otice… may be delayed if a law enforcement agency informs the person that notification may impede a criminal investigation or jeopardize national or homeland security, provided that such request by law enforcement is made in writing or the person documents such request contemporaneously in writing, including the name of the law enforcement officer making the request and the officer's law enforcement agency engaged in the investigation. The notice… shall be provided without unreasonable delay after the law enforcement agency communications to the person its determination that notice will no longer impede the investigation or jeopardize national or homeland security." "[N]otice to affected consumers shall be provided by one of the following methods: (a) Written notice; (b) Electronic notice for those consumers for whom the person has a valid email address and who have agreed to receive communications electronically, if the notice provided is consistent with [15 U.S.C. § 7001]; (c) Telephonic notice, if such contact is made directly with the affected consumers; or (d) Substitute notice, if: a. The person demonstrates that the cost of providing notice would exceed one hundred thousand dollars; or b. The class of affected consumers to be notified exceeds one hundred fifty thousand; or c. The person does not have sufficient contact information or consent to satisfy [the immediately above] paragraphs	

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	(a), (b), or (c)… for only those affected consumers without sufficient contact information or consent; or d. The person is unable to identify particular affected consumers, for only those unidentifiable consumers. (7) Substitute notice… shall consist of all the following: (a) Email notice when the person has an electronic mail address for the affected consumer; (b) Conspicuous posting of the notice or a link to the notice on the Internet website of the person if the person maintains an Internet website; and (c) Notification to major statewide media."	
Montana Mont. Code § 30-14-1702, §§ 30-14-1704 – 30-14-1705 (Oct. 1, 2015)	"A[] person or business that conducts business in Montana and that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the data system… to any resident of Montana whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. The disclosure must be made without unreasonable delay, consistent with… any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system… [but] notification… may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation and requests a delay in notification. [In this case, notice]… must be made after the law enforcement agency determines that it will not compromise the investigation." "[N]otice may be provided by one of the following methods: (i) written notice;	*(Not provided for.)*

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	(ii) electronic notice, if the notice provided is consistent with [15 U.S.C. § 7001]; (iii) telephonic notice; or (iv) substitute notice, if the person or business demonstrates that: (A) the cost of providing notice would exceed $250,000; (B) the affected class of subject persons to be notified exceeds 500,000; or (C) the person or business does not have sufficient contact information. (b) Substitute notice must consist of the following: (i) an electronic mail notice when the person or business has an electronic mail address for the subject persons; and (ii) conspicuous posting of the notice on the website page of the person or business if the person or business maintains one; or (iii) notification to applicable local or statewide media."	
Nebraska Neb. Rev. Stat. §§ 87-801 – 87-807 (Jul. 18, 2018)	"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 shall… give notice to the affected Nebraska resident. Notice shall be made as soon as possible and without unreasonable delay, consistent with… any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system… [but notice] may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation. Notice shall be made in good faith, without unreasonable delay, and as soon as possible after the law enforcement agency determines that notification will no longer impede the investigation."	*(Not provided for.)*

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	"An individual or a commercial entity that maintains computerized data that includes personal information about the individual or commercial entity does not own or license shall give notice to… the owner or licensee of the information of any breach of the security of the system when it becomes aware of a breach." "Notice means: (a) Written notice; (b) Telephonic notice; (c) Electronic notice, if the notice provided is consistent with [15 U.S.C. § 7001], as such section existed on January 1, 2006; (d) Substitute notice, if the individual or commercial entity… demonstrates that the cost of providing notice will exceed seventy-five thousand dollars, that the affected class of Nebraska residents to be notified exceeds one hundred thousand residents, or that the individual or commercial entity does not have sufficient contact information to provide notice. Substitute notice… requires all of the following: (i) Electronic mail notice if the individual or commercial entity has electronic mail addresses for the members of the affected class of Nebraska residents; (ii) Conspicuous posting of the notice on the web site of the individual or commercial entity if the individual or commercial entity maintains a web site; and (iii) Notice to major statewide media outlets." "[But in the case that] the individual or commercial entity… has ten employees or fewer and demonstrates that the cost of providing notice will exceed ten thousand dollars… [then] [s]ubstitute notice… [instead] requires all of the following:	

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	(i) Electronic mail notice if the individual or commercial entity has electronic mail addresses for the members of the affected class of Nebraska residents; (ii) Notification by a paid advertisement in a local newspaper that is distributed in the geographic area in which the individual or commercial entity is located, which advertisement shall be of sufficient size that it covers at least one-quarter of a page in the newspaper and shall be published in the newspaper at least once a week for three consecutive weeks; (iii) Conspicuous posting of the notice on the web site of the individual or commercial entity if the individual or commercial entity maintains a web site; and (iv) Notification to major media outlets in the geographic area in which the individual or commercial entity is located."	
Nevada Nev. Rev. Stat. §§ 603A.010 – 603A.100, §§ 603A.215 – 603A.290 (Oct. 1, 2021)	"[A] data collector that owns or licenses computerized data which includes personal information shall disclose any breach of the security of the system data following discovery or notification of the breach to any resident of this State whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement… or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system data." "Any data collector that maintains computerized data which includes personal information that the data collector does not own shall notify the owner or licensee of the	*(Not provided for.)*

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	information of any breach of the security of the system data immediately following discovery if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." "The notification required... may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification… must be made after the law enforcement agency determines that the notification will not compromise the investigation." "The notification… may be provided by one of the following methods: (a) Written notification. (b) Electronic notification, if the notification provided is consistent with 15 U.S.C. §§ 7001 et seq. (c) Substitute notification, if the data collector demonstrates that the cost of providing notification would exceed $250,000, the affected class of subject persons to be notified exceeds 500,000 or the data collector does not have sufficient contact information. Substitute notification must consist of all the following: (1) Notification by electronic mail when the data collector has electronic mail addresses for the subject persons. (2) Conspicuous posting of the notification on the Internet website of the data collector, if the data collector maintains an Internet website. (3) Notification to major statewide media."	
New Hampshire N.H. Rev. Stat. §§ 359-C:19 –	"[A] person doing business in this state who owns or licenses computerized data that includes personal information shall… notify the affected individuals as soon as possible."	"Notice… shall include at a minimum: (a) A description of the incident in general terms. (b) The approximate date of breach. (c) The type of personal information obtained as a result of the security breach.

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
359-C:21 (Jan. 1, 2007)	"[A] person or business that maintains computerized data that includes personal information that the person or business does not own shall notify… the owner or licensee of the information of any breach of the security of the data immediately following discovery." "Notification[s]… may be delayed if a law enforcement agency, or national or homeland security agency determines that the notification will impede a criminal investigation or jeopardize national or homeland security." "The notice… shall be provided by one of the following methods: (a) Written notice. (b) Electronic notice, if the agency or business' primary means of communication with affected individuals is by electronic means. (c) Telephonic notice, provided that a log of each such notification is kept by the person or business who notifies affected persons. (d) Substitute notice, if the person demonstrates that the cost of providing notice would exceed $5,000, that the affected class of subject individuals to be notified exceeds 1,000, or the person does not have sufficient contact information or consent to provide notice pursuant to [the immediately above] subparagraphs [(a), (b), (c)]. Substitute notice shall consist of all of the following: (1) E-mail notice when the person has an e-mail address for the affected individuals. (2) Conspicuous posting of the notice on the person's business website, if the person maintains one. (3) Notification to major statewide media.	(d) The telephonic contact information of the [reporting] person."

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	(e) Notice pursuant to the person's internal notification procedures maintained as part of an information security policy for the treatment of personal information."	
New Jersey N.J. Stat. § 56:8-161, § 56:8-163, §§ 56:8-165 – 56:8-166 (Sep. 1, 2019)	"[A] business that conducts business in New Jersey… that compiles or maintains computerized records that include personal information, shall disclose any breach of security of those computerized records… to any customer who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person. The disclosure to a customer shall be made in the most expedient time possible and without unreasonable delay, consistent with… any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system… [but notice] shall be delayed if a law enforcement agency determines that the notification will impede a criminal or civil investigation and that agency has made a request that the notification be delayed. The notification… shall be made after the law enforcement agency determines that its disclosure will not compromise the investigation and notifies that business." "[A] business… that compiles or maintains computerized records that include personal information on behalf of another business… shall notify that business… who shall notify its New Jersey customers, as provided [immediately above] of any breach of security of the computerized records immediately following discovery." "Notice may be provided by one of the following methods: (1) Written notice;	*(Not provided for.)*

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	(2) Electronic notice, if the notice provided is consistent with [15 U.S.C. § 7001]; or (3) Substitute notice, if the business… demonstrates that the cost of providing notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000, or the business… does not have sufficient contact information. Substitute notice shall consist of all of the following: (a) E-mail notice when the business… has an e-mail address; (b) Conspicuous posting of the notice on the Internet web site page of the business… if the business… maintains one; and (c) Notification to major Statewide media." "[I]n the case of a breach of security involving a user name or password, in combination with any password or security question and answer that would permit access to an online account, and no other personal information as defined in [N.J. Stat. § 56:8-161], the business… may provide the notification in electronic or other form that directs the customer whose personal information has been breached to promptly change any password and security question or answer, as applicable, or to take other appropriate steps to protect the online account with the business… and all other online accounts for which the customer uses the same user name or email address and password or security question or answer." "[A] business… that furnishes an email account shall not provide notification to the email account that is subject to a security breach. [In that case] [t]he business… shall provide notice by another method described [above] or by clear and conspicuous notice delivered to the customer	

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	online when the customer is connected to the online account from an Internet Protocol address or online location from which the business… knows the customer customarily accesses the account." "'Records' means any material, regardless of the physical form, on which information is recorded or preserved by any means, including written or spoken words, graphically depicted, printed, or electromagnetically transmitted… [but] does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed."	
New Mexico N.M. Stat. §§ 57-12C-1 – 57-12C-2, §§ 57-12C-6 – 57-12C-11 (Jun. 16, 2017)	"[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 forty-five calendar days following discovery of the security breach." "[A] 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 forty-five calendar days following discovery of the breach." "[N]otification[s]… may be delayed: A. if a law enforcement agency determines that the notification will impede a criminal investigation; or	"Notification [to individuals]… shall contain: A. the name and contact information of the notifying person; B. a list of the types of personal identifying information that are reasonably believed to have been the subject of a security breach, if known; C. the date of the security breach, the estimated date of the breach or the range of dates within which the security breach occurred, if known; D. a general description of the security breach incident; E. the toll-free telephone numbers and addresses of the major consumer reporting agencies; F. advice that directs the recipient to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach; and G. advice that informs the recipient of the notification of the recipient's rights pursuant to the federal Fair Credit Reporting [Act]."

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	B. as necessary to determine the scope of the security breach and restore the integrity, security and confidentiality of the data system." "A person… shall provide that notification by: (1) United States mail; (2) electronic notification, if the person required to make the notification primarily communicates with the New Mexico resident by electronic means or if the notice provided is consistent with [15 U.S.C. § 7001]; or (3) a substitute notification, if the person demonstrates that: (a) the cost of providing notification would exceed one hundred thousand dollars ($100,000); (b) the number of residents to be notified exceeds fifty thousand; or (c) the person does not have on record a physical address or sufficient contact information for the residents that the person or business is required to notify. "Substitute notification… shall consist of: (1) sending electronic notification to the email address of those residents for whom the person has a valid email address; (2) posting notification of the security breach in a conspicuous location on the website of the person… if the person maintains a website; and (3) sending written notification to the office of the attorney general and major media outlets in New Mexico."	
New York	"[A] person or business which owns or licenses computerized data which includes private information shall disclose any breach of the security of the system… to any	"[N]otice shall include contact information for the person or business making the notification, the telephone numbers and websites of the relevant state and federal agencies that provide information regarding security breach response and identity theft

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
N.Y. Gen. Bus. Law § 899-AA (Oct. 23, 2019)	resident of New York state whose private information was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with… any measures necessary to determine the scope of the breach and restore the integrity of the system… [but notice] may be delayed if a law enforcement agency determines that such notification impedes a criminal investigation. The notification… shall be made after such law enforcement agency determines that such notification does not compromise such investigation." "[A] person or business which maintains computerized data which includes private information which such person or business does not own shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery." "The notice… shall be directly provided to the affected persons by one of the following methods: (a) written notice; (b) electronic notice, provided that the person to whom notice is required has expressly consented to receiving said notice in electronic form and a log of each such notification is kept by the person or business who notifies affected persons in such form; provided further, however, that in no case shall any person or business require a person to consent to accepting said notice in said form as a condition of establishing any business relationship or engaging in any transaction. (c) telephone notification provided that a log of each such notification is kept by the person or business who notifies affected persons; or	prevention and protection information, and a description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so accessed or acquired."

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	(d) substitute notice, if a business demonstrates to the state attorney general that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or such business does not have sufficient contact information. Substitute notice shall consist of all of the following: (1) e-mail notice when such business has an e-mail address for the subject persons, except if the breached information includes an e-mail address in combination with a password or security question and answer that would permit access to the online account, in which case the person or business shall instead provide clear and conspicuous notice delivered to the consumer online when the consumer is connected to the online account from an internet protocol address or from an online location which the person or business knows the consumer customarily uses to access the online account; (2) conspicuous posting of the notice on such business's web site page, if such business maintains one; and (3) notification to major statewide media."	
North Carolina N.C. Gen. Stat. § 75-60, § 75-61, § 75-65 (Jan. 1, 2016)	"[A] 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) shall provide notice to the affected person that there has been a security breach… The disclosure notification shall be made without unreasonable delay, consistent with the legitimate needs of law enforcement… [and] any measures necessary to determine sufficient contact information, determine the scope of the breach	"The notice shall be clear and conspicuous… [and] shall include all of the following: (1) A description of the incident in general terms. (2) A description of the type of personal information that was subject to the unauthorized access and acquisition. (3) A description of the general acts of the business to protect the personal information from further unauthorized access. (4) A telephone number for the business that the person may call for further information and assistance, if one exists. (5) Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports. (6) The toll-free numbers and addresses for the major consumer reporting agencies.

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	and restore the reasonable integrity, security, and confidentiality of the data system." "[A] 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 shall notify the owner or licensee of the information of any security breach immediately following discovery of the breach, consistent with the legitimate needs of law enforcement." "[Consistent with the needs of law enforcement means that notice] shall be delayed if a law enforcement agency informs the business that notification may impede a criminal investigation or jeopardize national or homeland security, provided that such request is made in writing or the business documents such request contemporaneously in writing, including the name of the law enforcement officer making the request and the officer's law enforcement agency engaged in the investigation. The notice… shall be provided without unreasonable delay after the law enforcement agency communications to the business its determination that notice will no longer impede the investigation or jeopardize national or homeland security." "[N]otice to affected persons may be provided by one of the following methods: (1) Written notice. (2) Electronic notice, for those persons for whom it has a valid e-mail address and who have agreed to receive	(7) The toll-free numbers, addresses, and Web site addresses for the Federal Trade Commission and the North Carolina Attorney General's Office, along with a statement that the individual can obtain information from these sources about preventing identity theft." "'Consumer reporting agency'… [means a] person who, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties."

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	communications electronically if the notice provided is consistent with [15 U.S.C. § 7001]. (3) Telephonic notice provided that contact is made directly with the affected persons. (4) Substitute notice, if the business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000) or that the affected class of subject persons to be notified exceeds 500,000, or if the business does not have sufficient contact information or consent to satisfy [the immediately above] subdivisions (1), (2), or (3)… for only those affected persons without sufficient contact information or consent, or if the business is unable to identify particular affected persons, for only those unidentifiable affected persons. Substitute notice shall consist of all the following: a. E-mail notice when the business has an electronic mail address for the subject persons. b. Conspicuous posting of the notice on the Web site page of the business, if one is maintained. c. Notification to major statewide media."	
North Dakota N.D. Cent. Code §§ 51-30-01 – 51-30-07 (Aug. 1, 2015)	"[A] person that owns or licenses computerized data that includes personal information, shall disclose any breach of the security system… to any resident of the state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." "The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with… any measures necessary to determine the scope of the breach and to restore the integrity of the data system… [but notice] may be delayed if a law enforcement agency	*(Not provided for.)*

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	determines that the notification will impede a criminal investigation. The notification… must be made after the law enforcement agency determines that the notification will not compromise the investigation." "[A] person that maintains computerized data that includes personal information that the person does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following the discovery." "Notice… may be provided by one of the following methods: 1. Written notice; 2. Electronic notice, if the notice provided is consistent with [15 U.S.C. § 7001]; or 3. Substitute notice, if the person demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or the person does not have sufficient contact information. Substitute notice consists of the following: a. E-mail notice when the person has an e-mail address for the subject persons; b. Conspicuous posting of the notice on the person's website page, if the person maintains one; and c. Notification to major statewide media."	
Ohio Ohio Rev. Code §§ 1349.19 – 1349.192	"[A] person that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system… to any resident of this state whose personal information was, or reasonably is believed to have been, accessed and acquired by an unauthorized	*(Not provided for.)*

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
(Mar. 30, 2007)	person if [such] access and acquisition… causes or reasonably is believed will cause a material risk of identity theft or other fraud to the resident." "The person shall make the disclosure… in the most expedient time possible but not later than forty-five days following its discovery or notification of the breach in the security of the system… consistent with any measures necessary to determine the scope of the breach, including which residents' personal information was accessed and acquired, and to restore the reasonable integrity of the data system." "[A] person that, on behalf of or at the direction of another person… is the custodian of or stores computerized data that includes personal information shall notify that other person… of any breach of the security of the system in an expeditious manner." "The person may delay the disclosure or notification [otherwise] required… if a law enforcement agency determines that the disclosure or notification will impede a criminal investigation or jeopardize homeland or national security, in which case, the person shall make the disclosure or notification after the law enforcement agency determines that disclosure or notification will not compromise the investigation or jeopardize homeland or national security." "[A] person may disclose or make a notification by any of the following methods: (1) Written notice;	

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	(2) Electronic notice, if the person's primary method of communication with the resident to whom the disclosure must be made is by electronic means; (3) Telephone notice; (4) Substitute notice… if the person required to disclose demonstrates that the person does not have sufficient contact information to provide notice in a manner described in [the immediately above] division[s] [(1), (2), or (3)], or that the cost of providing disclosure or notice to residents… would exceed two hundred fifty thousand dollars, or that the affected class of subject residents… exceeds five hundred thousand persons. Substitute notice… shall consist [by default] of all of the following: (a) Electronic mail notice if the person has an electronic mail address for the resident to whom the disclosure must be made; (b) Conspicuous posting of the disclosure or notice on the person's web site, if the person maintains one; (c) Notification to major media outlets, to the extent that the cumulative total of the readership, viewing audience, or listening audience of all of the outlets so notified equals or exceeds seventy-five per cent of the population of this state. "[But in the case that] the person required to disclose demonstrates that the person is a business entity with ten employees or fewer and that the cost of providing the disclosures or notices to residents to whom disclosure or notification is required will exceed ten thousand dollars… [then] [s]ubstitute notice… shall consist of all of the following: (a) Notification by a paid advertisement in a local newspaper that is distributed in the geographic area in which the business entity is located, which advertisement	

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	shall be of sufficient size that it covers at least one-quarter of a page in the newspaper and shall be published in the newspaper at least once a week for three consecutive weeks; (b) Conspicuous posting of the disclosure or notice on the business entity's web site, if the entity maintains one; (c) Notification to major media outlets in the geographic area in which the business entity is located."	
Oklahoma Okla. Stat. tit. 24, §§ 161 – 166 (Nov. 1, 2008)	"An individual or entity that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system… to any resident of this state whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person and that causes, or the individual or entity reasonably believes has caused or will cause, identity theft or other fraud to any resident of this state… without unreasonable delay." "[But notice may be delayed] to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the system… [or] if a law enforcement agency determines and advises the individual or entity that the notice will impede a criminal or civil investigation or homeland or national security. Notice… must be made without unreasonable delay after the law enforcement agency determines that notification will no longer impede the investigation or jeopardize national or homeland security." "An individual or entity that maintains computerized data that includes personal information that the individual or entity does not own or license shall notify the owner or	*(Not provided for.)*

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	licensee of the information of any breach of the security of the system as soon as practicable following discovery." "'Notice' means: a. written notice to the postal address in the records of the individual or entity, b. telephone notice, c. electronic notice, or d. substitute notice, if the individual or the entity required to provide notice demonstrates that the cost of providing notice will exceed Fifty Thousand Dollars ($50,000.00), or that the affected class of residents to be notified exceeds one hundred thousand (100,000) persons, or that the individual or the entity does not have sufficient contact information or consent to provide notice as described in [the immediately above] subparagraph[s] a, b or c… Substitute notice consists of any two of the following: (1) e-mail notice if the individual or the entity has e-mail addresses for the members of the affected class of residents, (2) conspicuous posting of the notice on the Internet web site of the individual or the entity if the individual or the entity maintains a public Internet web site, or (3) notice to major statewide media."	
Oregon Or. Rev. Stat. §§ 646A.600 – 646A.604, 646A.624 – 646A.628 (Jan. 1, 2020)	"[A] covered entity shall give notice of the breach of security to… [t]he consumer to whom the personal information pertains… in the most expeditious manner possible, without unreasonable delay, but not later than 45 days after discovering or receiving notification of the breach of security." "'Consumer' means an individual resident of this state."	"Notice… must include, at a minimum: (a) A description of the breach of security in general terms; (b) The approximate date of the breach of security; (c) The type of personal information that was subject to the breach of security; (d) Contact information for the covered entity; (e) Contact information for national consumer reporting agencies; and (f) Advice to the consumer to report suspected identity theft to law enforcement, including the Attorney General and the Federal Trade Commission."

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	"A vendor… shall notify a covered entity with which the vendor has a contract as soon as is practicable but not later than 10 days after discovering the breach of security or having a reason to believe that the breach of security occurred." "[A] vendor [that] has a contract with another vendor that, in turn, has a contract with a covered entity… shall notify the other vendor of a breach of security as [soon as is practicable but not later than 10 days after discovering the breach of security or having a reason to believe that the breach of security occurred]." "Before providing the [individual] notice… a covered entity shall undertake reasonable measures that are necessary to: (A) Determine sufficient contact information for the intended recipient of the notice; (B) Determine the scope of the breach of security; and (C) Restore the reasonable integrity, security and confidentiality of the personal information." "A covered entity may delay giving the notice… only if a law enforcement agency determines that a notification will impede a criminal investigation and if the law enforcement agency requests in writing that the covered entity delay the notification." "A covered entity may notify a consumer of a breach of security: (a) In writing; (b) Electronically, if the covered entity customarily communicates with the consumer electronically or if the notice is consistent with [15 U.S.C. § 7001] as [it] existed on January 1, 2020;	"'Consumer reporting agency' means a consumer reporting agency as described in [15 U.S.C. § 1681a(p)] as that [section] existed on January 1, 2020."

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	(c) By telephone, if the covered entity contacts the affected consumer directly; or (d) With substitute notice, if the covered entity demonstrates that the cost of notification otherwise would exceed $250,000 or that the affected class of consumers exceeds 350,000, or if the covered entity does not have sufficient contact information to notify affected consumers… [Here], "substitute notice" means: (A) Posting the notice or a link to the notice conspicuously on the covered entity's website if the covered entity maintains a website; and (B) Notifying major statewide television and newspaper media."	
Pennsylvania 73 Pa. Cons. Stat. §§ 2301 – 2330 (May 2, 2023)	"An entity that maintains, stores or manages computerized data that includes personal information shall provide notice of any breach of the security of the system following determination of the breach of the security of the system to any resident of this Commonwealth whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person… without unreasonable delay… [considering time needed] to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system." "[But notice] may be delayed if a law enforcement agency determines and advises the entity in writing specifically referencing [Pa. Cons. Stat. § 2304] that the notification will impede a criminal or civil investigation. The notification… shall be made after the law enforcement agency determines that it will not compromise the investigation or national or homeland security."	"[Telephonic] notice… [must be] given in a clear and conspicuous manner, [describe] the incident in general terms and verif[y] personal information but does not require the customer to provide personal information and the customer is provided with a telephone number to call or Internet website to visit for further information or assistance." "[Electronic notice] in the case of a breach… involving personal information for a user name or e-mail address in combination with a password or security question and answer that would permit access to an online account, the entity, to the extent that it has sufficient contact information for the person, may comply with this section by providing the breach of the security of the system notification in electronic or other form that directs the person whose personal information has been materially compromised by the breach of the security of the system to promptly change the person's password and security question or answer, as applicable or to take other steps appropriate to protect the online account with the entity and other online accounts for which the person whose personal information has been materially compromised by the breach of the security of the system uses the same user name or e-mail address and password or security question or answer."

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	"A vendor that maintains, stores or manages computerized data on behalf of another entity shall provide notice of any breach of the security of the system… to the entity on whose behalf the vendor maintains, stores, or manages the data." "'Notice' may be provided by any of the following methods of notification: (1) Written notice to the last known home address for the individual. (2) Telephonic notice, if the individual can be reasonably expected to receive it and… verifies personal information but does not require the individual to provide personal information and the individual is provided with a telephone number to call or Internet website to visit for further information or assistance. (3) E-mail notice, if a prior business relationship exists and the person or entity has a valid e-mail address for the individual. (3.1) Electronic notice, if the notice directs the person whose personal information has been materially compromised by a breach of the security of the system to promptly change the person's password and security question or answer, as applicable, or to take other steps appropriate to protect the person's online account to the extent the entity has sufficient contact information for the person. (4)(i) Substitute notice, if the entity demonstrates one of the following: (A) The cost of providing notice would exceed $100,000. (B) The affected class of subject persons to be notified exceeds 175,000. (C) The entity does not have sufficient contact information.	

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	(ii) Substitute notice shall consist of all of the following: (A) E-mail notice when the entity has an e-mail address for the subject persons. (B) Conspicuous posting of the notice on the entity's Internet website if the entity maintains one. (C) Notification to major Statewide media."	
Rhode Island R.I. Gen. Laws § 11-49.3-1, §§ 11-49.3-3 – 11-49.3-6 (Jul. 2, 2016)	"[A] person that stores, owns, collects, processes, maintains, acquires, uses, or licenses data that includes personal information shall provide notification… to any resident of Rhode Island whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person or entity." "The notification shall be made in the most expedient time possible, but no later than forty-five (45) calendar days after confirmation of the breach and the ability to ascertain the information required to fulfill the notice [content] requirements… [but notice] may be delayed if a federal, state, or local law enforcement agency determines that the notification will impede a criminal investigation. The federal, state, or local law enforcement agency must notify the… person of the request to delay notification without unreasonable delay. If notice is delayed due to such determination, then, as soon as the federal, state, or municipal law enforcement agency determines and informs the… person that notification no longer poses a risk of impeding an investigation, notice shall be provided as soon as practicable." "'[N]otice' may be provided by one of the following methods: (1) Written notice;	"The notification to individuals must include the following information to the extent known: (1) A general and brief description of the incident, including how the security breach occurred and the number of affected individuals; (2) The type of information that was subject to the breach; (3) Date of breach, estimated date of breach, or the date range within which the breach occurred; (4) Date that the breach was discovered; (5) A clear and concise description of any remediation services offered to affected individuals including toll free numbers and websites to contact: (i) The credit reporting agencies; (ii) Remediation service providers; (iii) The attorney general; and (6) A clear and concise description of the consumer's ability to file or obtain a police report; how a consumer requests a security freeze and the necessary information to be provided when requesting the security freeze; and that fees may be required to be paid to the consumer reporting agencies."

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	(2) Electronic notice, if the notice provided is consistent with [15 U.S.C. § 7001]; (3) Substitute notice, if the… person demonstrates that the cost of providing notice would exceed twenty-five thousand dollars ($25,000), or that the affected class of subject persons to be notified exceeds fifty thousand (50,000), or the… person does not have sufficient contact information. Substitute notice shall consist of all of the following: (A) E-mail notice when the… person has an e-mail address for the subject persons; (B) Conspicuous posting of the notice on the… person's website page, if the… person maintains one; (C) Notification to major statewide media."	
South Carolina S.C. Code § 39-1-90 (Apr. 23, 2013)	"A person conducting business in this State, and owning or licensing computerized data or other data that includes personal identifying information, shall disclose a breach of the security of the system… to a resident of this State whose personal identifying information that was not rendered unusable through encryption, redaction, or other methods was, or is reasonably believed to have been, acquired by an unauthorized person when the illegal use of the information has occurred or is reasonably likely to occur or use of the information creates a material risk of harm to the resident. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with… measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system… [but notice] may be delayed if a law enforcement agency determines that the notification impedes a criminal investigation. The notification… must be made after the law enforcement	*(Not provided for.)*

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	agency determines that it no longer compromises the investigation." "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 shall notify the owner or licensee of the information of a breach of the security of the data immediately following discovery." "The notice… may be provided by: (1) written notice; (2) electronic notice, if the person's primary method of communication with the individual is by electronic means or is consistent with [15 U.S.C. § 7001] and [S.C. Code §§ 11-6-1 et seq.]; (3) telephonic notice; or (4) substitute notice, if the person demonstrates that the cost of providing notice exceeds two hundred fifty thousand dollars or that the affected class of subject persons to be notified exceeds five hundred thousand or the person has insufficient contact information. Substitute notice consists of: (a) e-mail notice when the person has an e-mail address for the subject persons; (b) conspicuous posting of the notice on the web site page of the person, if the person maintains one; or (c) notification to major statewide media."	
South Dakota S.D. Cod. Laws §§ 22-40-19 – 22-40-26	"[A]n 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	*(Not provided for.)*

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
(Jul. 1, 2018)	person. A disclosure… shall be made not later than sixty days from the discovery or notification of the breach of system security, unless a longer period of time is required due to the legitimate needs of law enforcement." "[The legitimate needs of law enforcement means that notice] may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. If the notification is delayed, the notification shall be made not later than thirty days after the law enforcement agency determines that notification will not compromise the criminal investigation." "A disclosure… may be provided by: (1) Written notice; (2) Electronic notice, if the electronic notice is consistent with [15 U.S.C. § 7001] in effect as of January 1, 2018, or if the information holder's primary method of communication with the resident of this state has been by electronic means; or (3) Substitute notice, if the information holder demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars, that the affected class of persons to be notified exceeds five hundred thousand persons, or that the information holder does not have sufficient contact information and the notice consists of each of the following: (a) Email notice, if the information holder has an email address for the subject persons; (b) Conspicuous posting of the notice on the information holder's website, if the information holder maintains a website page; and (c) Notification to statewide media."	

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
Tennessee Tenn. Code § 47-18-2107 (Apr. 4, 2017)	"[T]he information holder shall disclose the breach of system security to any resident of this state whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made no later than forty-five (45) days from the discovery or notification of the breach of system security, unless a longer period of time is required due to the legitimate needs of law enforcement." "[An] information holder that maintains computerized data that includes personal information that the information holder does not own shall notify the owner or licensee of the information of any breach of system security… The disclosure must be made no later than forty-five (45) days from the discovery or notification of the breach of system security, unless a longer period of time is required due to the legitimate needs of law enforcement." "[Here, the legitimate needs of law enforcement allow notice to] be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. If the notification is delayed, it must be made no later than forty-five (45) days after the law enforcement agency determines that notification will not compromise the investigation." "[N]otice may be provided by one (1) of the following methods: (1) Written notice; (2) Electronic notice, if the notice provided is consistent with [15 U.S.C. § 7001] or if the information holder's primary method of communication with the resident of this state has been by electronic means; or	*(Not provided for.)*

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	(3) Substitute notice, if the information holder demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), that the affected class of subject persons to be notified exceeds five hundred thousand (500,000), or the information holder does not have sufficient contact information. and the [substitute] notice consists of all of the following: (A) E-mail notice, when the information holder has an e-mail address for the subject persons; (B) Conspicuous posting of the notice on the information holder's internet website page, if the information holder maintains such website page; and (C) Notification to major statewide media."	
Texas Tex. Bus. & Com. Code § 521.002, § 521.053, § 521.151 (As amended by SB 768, effective Sep. 1, 2023)	"A person who conducts business in this state and owns or licenses computerized data that includes sensitive personal information shall disclose any breach of system security… to any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made without unreasonable delay and in each case not later than the 60th day after the date on which the person determines that the breach occurred, except… as necessary to determine the scope of the breach and restore the reasonable integrity of the data system." "If the individual whose sensitive personal information was or is reasonably believed to have been acquired by an unauthorized person is a resident of a state that requires a person [who conducts business in this state and owns or licenses computerized data that includes sensitive personal information] to provide notice of a breach of system security, the notice of the breach of system security	*(Not provided for.)*

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	required under [this law] may be provided under that state's law or under [this law]." "[A] person who maintains computerized data that includes sensitive personal information not owned by the person shall notify the owner or license holder of the information of any breach of system security immediately after discovering the breach." "A person may delay providing notice… [to affected individuals] or [to the owner or license holder of the information] at the request of a law enforcement agency that determines that the notification will impede a criminal investigation. The notification shall be made as soon as the law enforcement agency determines that the notification will not compromise the investigation." "A person may give notice… [to affected individuals or the owner or license holder of the information] by providing: (1) written notice at the last known address of the individual; (2) electronic notice, if the notice is provided in accordance with [15 U.S.C. § 7001]; or (3) [substitute] notice." "(f) [Substitute notice is permitted] [i]f the person… demonstrates that the cost of providing notice would exceed $250,000, the number of affected persons exceeds 500,000, or the person does not have sufficient contact information, [and] the [substitute] notice may be given by: (1) electronic mail, if the person has electronic mail addresses for the affected persons; (2) conspicuous posting of the notice on the person's website; or	

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	(3) notice published in or broadcast on major statewide media."	
Utah Utah Code §§ 13-44-101 – 13-44-103, § 13-44-202, § 13-44-301 (May 3, 2023)	"A person who owns or license computerized data that includes personal information concerning a Utah resident shall…provide notification [of a breach] to each affected Utah resident… in the most expedient time possible without unreasonable delay: (a) considering legitimate investigative needs of law enforcement…, (b) after determining the scope of the breach of system security; and (c) after restoring the reasonable integrity of the system." "[Legitimate investigative needs of law enforcement allow] a person… [to] delay providing notification…at the request of a law enforcement agency that determines that notification may impede a criminal investigation. [In this case] [the] person… shall provide notification in good faith without unreasonable delay in the most expedient time possible after the law enforcement agency informs the person that notification will no longer impede the criminal investigation." "A person who maintains computerized data that includes personal information that the person does not own or license shall notify… the owner or licensee of the information of any breach of system security immediately following the person's discovery of the breach." "A notification… may be provided: (i) in writing by first-class mail to the most recent address the person has for the resident;	*(Not provided for.)*

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	(ii) electronically, if the person's primary method of communication with the resident is by electronic means, or if provided in accordance with [15 U.S.C. § 7001]; (iii) by telephone, including through the use of automatic dialing technology not prohibited by other law; or (iv) for residents of the state for whom notification in a manner described in [the immediately above subsections (i), (ii), (iii)] is not feasible, by publishing notice of the breach of system security: (A) in a newspaper of general circulation; and (B) as required in [Utah Code § 45-1-101]."	
Vermont Vt. Stat. tit. 9, § 2430, § 2435 (Jul. 1, 2020)	"[A] data collector that owns or licenses computerized personally identifiable information or login credentials shall notify the consumer that there has been a security breach... Notice of the security breach shall be made in the most expedient time possible and without unreasonable delay, but not later than 45 days after the discovery or notification, consistent with the legitimate needs of the law enforcement agency… or with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system." "'Consumer' means an individual residing in this State." "[A] data collector that maintains or possesses computerized data containing personally identifiable information or login credentials 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 or login credentials that the data collector	"The notice to a consumer… shall be clear and conspicuous. A notice to a consumer of a security breach involving personally identifiable information shall include a description of the following, if known to the data collector: (A) the incident in general terms; (B) the type of personally identifiable information that was subject to the security breach; (C) the general acts of the data collector to protect the personally identifiable information from further security breach; (D) a telephone number, toll-free if available, that the consumer may call for further information and assistance; (E) advice that directs the consumer to remain vigilant by reviewing account statements and monitoring free credit reports; and (F) the approximate date of the security breach." "If a security breach is limited to an unauthorized acquisition of login credentials for an online account other than an e-mail account the data collector… shall advise the consumer to take steps necessary to protect the online account, including to change his or her login credentials for the account and for any other account for which the consumer uses the same login credentials."

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	does not own or license shall notify the owner or licensee of the information of any security breach immediately following discovery of the breach, consistent with the legitimate needs of law enforcement." "[The legitimate needs of law enforcement means that] [t]he notice to a consumer… shall be delayed upon request of a law enforcement agency. A law enforcement agency may request the delay if it believes that notification may impede a law enforcement investigation, or a national or Homeland Security investigation, or jeopardize public safety or national or Homeland Security interests. In the event law enforcement makes the request for a delay in a manner other than in writing, the data collector shall document such request contemporaneously in writing, including the name of the law enforcement officer making the request and the officer's law enforcement agency engaged in the investigation. A law enforcement agency shall promptly notify the data collector in writing when the law enforcement agency no longer believes that notification may impede a law enforcement investigation, or a national or Homeland Security investigation, or jeopardize public safety or national or Homeland Security interests. The data collector shall provide notice… without unreasonable delay upon receipt of a written communication, which includes facsimile or electronic communication, from the law enforcement agency withdrawing its request for delay." "A data collector may provide notice of a security breach involving personally identifiable information to a consumer by one or more of the following methods: (A) Direct notice to consumers, which may be by one of the following methods:	

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	(i) written notice mailed to the consumer's residence; (ii) electronic notice, for those consumers for whom the data collector has a valid e-mail address if: (I) the data collector's primary method of communication with the consumer is by electronic means, the electronic notice does not request or contain a hypertext link to a request that the consumer provide personal information, and the electronic notice conspicuously warns consumers not to provide personal information in response to electronic communications regarding security breaches; or (II) the notice is consistent with [15 U.S.C. § 7001]; or (iii) telephonic notice, provided that telephonic contact is made directly with each affected consumer and not through a prerecorded message. (B)(i) Substitute notice if: (I) the data collector demonstrates that the lowest cost of providing [direct] notice to affected consumers… among written, e-mail, or telephonic notice would exceed $10,000.00; or (II) the data collector does not have sufficient contact information. "A data collector shall provide substitute notice by: (I) conspicuously posting the notice on the data collector's website if the data collector maintains one; and (II) notifying major statewide and regional media." "If a security breach is limited to an unauthorized acquisition of login credentials for an online account other than an e-mail account the data collector shall provide notice of the security breach to the consumer electronically or through one or more of the methods [of lawful direct or substitute notice]."	

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	"If a security breach is limited to an unauthorized acquisition of login credentials for an email account… the data collector shall not provide notice of the security breach through the email account… [and instead] provide notice of the security breach through one or more of the methods [of lawful direct or substitute notice]… or by clear and conspicuous notice delivered to the consumer online when the consumer is connected to the online account from an Internet protocol address or online location from which the data collector knows the consumer customarily accesses the account."	
Virginia Va. Code § 18.2-186.6 (Jul. 1, 2020)	"[A]n individual or entity that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system… [to] any affected resident of the Commonwealth without unreasonable delay. Notice… may be reasonably delayed to allow the individual or entity to determine the scope of the breach of the security of the system and restore the reasonable integrity of the system… [or] if, after the individual or entity notifies a law-enforcement agency, the law-enforcement agency determines and advises the individual or entity that the notice will impede a criminal or civil investigation, or homeland or national security. Notice shall be made without unreasonable delay after the law-enforcement agency determines that the notification will no longer impede the investigation or jeopardize national or homeland security." "An individual or entity that maintains computerized data that includes personal information that the individual or entity does not own or license shall notify the owner or licensee of the information of any breach of the security of	"Notice… shall include a description of the following: (1) The incident in general terms; (2) The type of personal information that was subject to the unauthorized access and acquisition; (3) The general acts of the individual or entity to protect the personal information from further unauthorized access; (4) A telephone number that the person may call for further information and assistance, if one exists; and (5) Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports."

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	the system without unreasonable delay following discovery of the breach of the security of the system." "A [data] processor shall adhere to the instructions of a [data] controller and shall assist the controller in meeting its obligations… includ[ing]… taking into account the nature of processing and the information available to the processor, by assisting the controller in meeting the controller's obligations in relation to… the notification of a breach of security of the system of the processor." "'Notice' means: 1. Written notice to the last known postal address in the records of the individual or entity; 2. Telephone notice; 3. Electronic notice; or 4. Substitute notice, if the individual or the entity required to provide notice demonstrates that the cost of providing notice will exceed $50,000, the affected class of Virginia residents to be notified exceeds 100,000 residents, or the individual or the entity does not have sufficient contact information or consent to provide notice as described in [the immediately above] subdivisions 1, 2, or 3… Substitute notice consists of all of the following: a. E-mail notice if the individual or the entity has e-mail addresses for the members of the affected class of residents; b. Conspicuous posting of the notice on the website of the individual or the entity if the individual or the entity maintains a website; and c. Notice to major statewide media."	

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	"'[Data] [c]ontroller' means the natural or legal person that, alone or jointly with others, determines the purpose and means of processing personal [information]." "'[Data] [p]rocessor' means a natural or legal entity that processes personal [information] on behalf of a [data] controller." "'Process' or 'processing' means any operation or set of operations performed, whether by manual or automated means… such as the collection, use, storage, disclosure, analysis, deletion, or modification."	
Washington Wash. Rev. Code §§ 19.255.005 – 19.255.040 (Mar. 1, 2020)	"[A] person or business that conducts business in this state and that owns or licenses data that includes personal information shall disclose any breach of the security of the system to any resident of this state whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the personal information was not secured." "[A] person or business that maintains or possesses data that may include personal information that the person or business does not own or license shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery." "Notification to affected consumers… must be made in the most expedient time possible, without unreasonable delay, and no more than thirty calendar days after the breach was discovered, unless the delay is… due to any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system… [or	"[A] person or business that is required to issue notification… shall meet all of the following requirements: (a) The notification must be written in plain language; and (b) The notification must include, at a minimum, the following information: (i) The name and contact information of the reporting person or business…; (ii) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach; (iii) A time frame of exposure, if known, including the date of the breach and the date of the discovery of the breach; and (iv) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed personal information." "If the breach of the security of the system involves personal information including a user name or password… [the] notice… must inform the person whose personal information has been breached to promptly change his or her password and security question or answer, as applicable, or to take other appropriate steps to protect the online account with the person or business and all other online accounts for which the person whose personal information has been breached uses the same user name or email address and password or security question or answer."

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	unless] the data owner or licensee contacts a law enforcement agency after discovery of a breach of the security of the system and a law enforcement agency determines that the notification will impede a criminal investigation. [In the latter case,] [t]he notification… shall be made after the law enforcement agency determines that it will not compromise the investigation." "[N]otice may be provided by one of the following methods: (a) Written notice; (b) Electronic notice, if the notice provided is consistent with [15 U.S.C. § 7001]; or (c) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following: (i) E-mail notice when the person or business has an e-mail address for the subject persons; (ii) Conspicuous posting of the notice on the web site page of the person or business, if the person or business maintains one; and (iii) Notification to major statewide media." "If the breach of the security of the system involves personal information including a user name or password, notice may be provided electronically or by email." "[If] the breach of the security of the system involves login credentials of an email account furnished by the person or business, the person or business may not provide the	"[If] the breach of the security of the system involves login credentials of an email account furnished by the person or business… [the notice] must inform the person whose personal information has been breached to promptly change his or her password and security question or answer, as applicable, or to take other appropriate steps to protect the online account with the person or business and all other online accounts for which the person whose personal information has been breached uses the same user name or email address and password or security question or answer."

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	notification to that email address, [and instead] must provide notice using another method [permitted above]."	
West Virginia W. Va. Code §§ 46A-2A-101 – 46A-2A-105 (Jun. 7, 2008)	"An individual or entity that owns or licenses computerized data that includes personal information shall give notice of any breach of the security of the system… to any resident of this state whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person and that causes, or the individual or entity reasonably believes has or will cause, identity theft or other fraud to any resident of this state. Except… in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the system, the notice shall be made without unreasonable delay… [but notice] may be delayed if a law-enforcement agency determines and advises the individual or entity that the notice will impede a criminal or civil investigation or homeland or national security. Notice… must be made without unreasonable delay after the law-enforcement agency determines that notification will no longer impede the investigation or jeopardize national or homeland security." "An individual or entity that maintains computerized data that includes personal information that the individual or entity does not own or license shall give notice to the owner or licensee of the information of any breach of the security of the system as soon as practicable following discovery." "'Notice' means: (A) Written notice to the postal address in the records of the individual or entity;	"The notice shall include: (1) To the extent possible, a description of the categories of information that were reasonably believed to have been accessed or acquired by an unauthorized person, including social security numbers, driver's licenses or state identification numbers and financial data; (2) A telephone number or website address that the individual may use to contact the entity or the agent of the entity and from whom the individual may learn: (A) What types of information the entity maintained about that individual or about individuals in general; and (B) Whether or not the entity maintained information about that individual. (3) The toll-free contact telephone numbers and addresses for the major credit reporting agencies and information on how to place a fraud alert or security freeze."

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	(B) Telephonic notice; (C) Electronic notice, if the notice provided is consistent with [15 U.S.C. § 7001]. (D) Substitute notice, if the individual or the entity… demonstrates that the cost of providing notice will exceed $50,000 or that the affected class of residents to be notified exceeds one hundred thousand persons or that the individual or the entity does not have sufficient contact information or to provide notice as described in [the immediately above] paragraph[s] (A), (B) or (C). Substitute notice consists of any two of the following: (i) E-mail notice if the individual or the entity has e-mail addresses for the members of the affected class of residents; (ii) Conspicuous posting of the notice on the website of the individual or the entity if the individual or the entity maintains a website; or (iii) Notice to major statewide media."	
Wisconsin Wis. Stat. §§ 134.98 – 134.99 (Mar. 28, 2008)	"[A]n entity whose principal place of business is located in this state or an entity that maintains or licenses personal information in this state… shall make reasonable efforts to notify each subject of the personal information." "[A]n entity whose principal place of business is not located in this state… shall make reasonable efforts to notify each resident of this state who is the subject of the personal information." "[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… shall notify	"The notice [from an entity whose principal place of business is located in this state or an entity that maintains or licenses personal information in this state] shall indicate that the entity knows of the unauthorized acquisition of personal information pertaining to the subject of the personal information." "The notice [from an entity whose principal place of business is not located in this state] shall indicate that the entity knows of the unauthorized acquisition of personal information pertaining to the resident of this state who is the subject of the personal information." "Upon written request by a person who has received a notice [from an entity whose principal place of business is located in this state or an entity that maintains or licenses personal information in this state] or [from an entity whose principal place of business is not located in this state], the entity that provided the notice shall identify the personal information that was acquired."

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	the person that owns or licenses the personal information of the acquisition as soon as practicable." "[A]n entity shall provide the notice… a reasonable time, not to exceed 45 days after the entity learns of the acquisition of personal information. A determination as to reasonableness… shall include consideration of the number of notices that an entity must provide and the methods of communication available to the entity." "A law enforcement agency may, in order to protect an investigation or homeland security, ask an entity not to provide a notice that is otherwise required… for any period of time and the notification process… shall begin at the end of that time period… if an entity receives [a law enforcement] request, the entity may not provide notice of or publicize an unauthorized acquisition of personal information, [until]… authorized by the law enforcement agency that made the request." "An entity shall provide the notice… by mail or by a method the entity has previously employed to communicate with the subject of the personal information. If an entity cannot with reasonable diligence determine the mailing address of the subject of the personal information, and if the entity has not previously communicated with the subject of the personal information, the entity shall provide notice by a method reasonably calculated to provide actual notice to the subject of the personal information."	
Wyoming	"An individual or commercial entity that conducts business in Wyoming and that owns or licenses computerized data that includes personal identifying information about a	"Notice… shall be clear and conspicuous and shall include, at a minimum: (i) A toll-free number: (A) That the individual may use to contact the person collecting the data, or his agent; and

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
Wyo. Stat. §§ 40-12-501 – 40-12-502 (Jul. 1, 2015) Wyo. Stat. § 6-3-901(b)(iii)–(xiv) (Jul. 1, 2015)	resident of Wyoming shall… give notice as soon as possible to the affected Wyoming resident. Notice shall be made in the most expedient time possible and without unreasonable delay, consistent with… any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system… [but notice] may be delayed if a law enforcement agency determines in writing that the notification may seriously impede a criminal investigation." "[A] person who maintains computerized data that includes personal identifying information on behalf of another business entity shall disclose to the business entity for which the information is maintained any breach of the security of the system as soon as practicable." "[N]otice to consumers may be provided by one (1) of the following methods: (i) Written notice; (ii) Electronic mail notice; (iii) Substitute notice, if the person demonstrates: (A) That the cost of providing notice would exceed ten thousand dollars ($10,000.00) for Wyoming-based persons or businesses, and two hundred fifty thousand dollars ($250,000.00) for all other businesses operating but not based in Wyoming; (B) That the affected class of subject persons to be notified exceeds ten thousand (10,000) for Wyoming-based persons or businesses and five hundred thousand (500,000) for all other businesses operating but not based in Wyoming; or (C) The person does not have sufficient contact information. (iv) Substitute notice shall consist of all of the following:	(B) From which the individual may learn the toll-free contact telephone numbers and addresses for the major credit reporting agencies. (ii) The types of personal identifying information that were or are reasonably believed to have been the subject of the breach; (iii) A general description of the breach incident; (iv) The approximate date of the breach of security, if that information is reasonably possible to determine at the time notice is provided; (v) In general terms, the actions taken by the individual or commercial entity to protect the system containing the personal identifying information from further breaches; (vi) Advice that directs the person to remain vigilant by reviewing account statements and monitoring credit reports; (vii) Whether notification was delayed as a result of a law enforcement investigation, if that information is reasonably possible to determine at the time the notice is provided." "[Substitute] notice to media shall include a toll-free phone number where an individual can learn whether or not that individual's personal data is included in the security breach."

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	(A) Conspicuous posting of the notice on the Internet, the World Wide Web or a similar proprietary or common carrier electronic system site of the person collecting the data, if the person maintains a public Internet, the World Wide Web or a similar proprietary or common carrier electronic system site; and (B) Notification to major statewide media." "'Substitute notice' means: (A) An electronic mail notice when the person or business has an electronic mail address for the subject persons; (B) Conspicuous posting of the notice on the website page of the person or business if the person or business maintains one; and (C) Publication in applicable local or statewide media."	
District of Columbia D.C. Code §§ 28-3851 – 28-3853 (Jun. 17, 2020)	"[A] 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… shall promptly notify any District of Columbia resident whose personal information was included in the breach. The notification shall be made in the most expedient time possible and without unreasonable delay, consistent with… any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system… [but notice] may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation but shall be made as soon as possible after the law enforcement agency determines that the notification will not compromise the investigation."	"The notification… shall include: (1) To the extent possible, a description of the categories of information that were, or are reasonably believed to have been, acquired by an unauthorized person, including the elements of personal information that were, or are reasonably believed to have been, acquired; (2) Contact information for the person or entity making the notification, including the business address, telephone number, and toll-free telephone number if one is maintained; (3) The toll-free telephone numbers and addresses for the major consumer reporting agencies, including a statement notifying the resident of the right to obtain a security freeze free of charge pursuant to 15 U.S.C. § 1681c-1 and information how a resident may request a security freeze; and (4) The toll-free telephone numbers, addresses, and website addresses for the following entities, including a statement that an individual can obtain information from these sources about steps to take to avoid identity theft: (A) The Federal Trade Commission; and (B) The Office of the Attorney General for the District of Columbia."

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	"[A] 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 shall notify the owner or licensee of the information of any breach of the security of the system in the most expedient time possible following discovery." "'Notify' or 'notification' means providing information through any of the following methods: (A) Written notice; (B) Electronic notice, if the customer has consented to receipt of electronic notice consistent with [15 U.S.C. § 7001], approved June 30, 2000…; or (C) (i) Substitute notice, if the person or entity demonstrates that the cost of providing notice… would exceed $50,000, that the number of persons to receive [individual] notice… exceeds 100,000, or that the person or entity does not have sufficient contact information. (ii) Substitute notice shall consist of all of the following (I) E-mail notice when the person or entity has an e-mail address for the subject persons; (II) Conspicuous posting of the notice on the website page of the person or business if the person or entity maintains one; and (III) Notice to major local and, if applicable, national media." "[I]n the case of a breach of the security of the system that only involves personal information [that is a user name or e-mail address in combination with a password, security question and answer, or other means of authentication, or any combination of personal information data elements that permits access to an individual's e-mail account], the person or entity may… provid[e] the notification in	"When a person or entity experiences a breach of the security of the system that requires notification … and such breach includes or is reasonably believed to include a social security number or taxpayer identification number, the person or entity shall offer to each District resident whose social security number or tax identification number was released identity theft protection services at no cost to such District resident for a period of not less than 18 months. The person or entity that experienced the breach of the security of its system shall provide all information necessary for District residents to enroll in the services required under this section." "[I]n the case of a breach of the security of the system that only involves personal information [that is a user name or e-mail address in combination with a password, security question and answer, or other means of authentication, or any combination of personal information data elements that permits access to an individual's e-mail account], [and] the person or entity… provid[es] the notification in electronic format or other form… [then the notice must direct]… the person to change the person's password and security question or answer, as applicable, or to take other steps appropriate to protect the e-mail account with the person or entity and all other online accounts for which the person whose personal information has been breached uses the same username or email address and password or security question or answer."

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	electronic format or other form that [meets the content requirements for such a breach]." "Notice [to individuals]… may be given by electronic mail if the person or entity's primary method of communication with the resident is by electronic means."	
Guam 9 Guam Code §§ 48.20 – 48.50 (Jul. 11, 2009)	"An individual or entity that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system… to any resident of Guam whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person and that causes, or the individual or entity reasonably believes has caused or will cause, identity theft or other fraud to any resident of Guam. Except… in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the system, the disclosure shall be made without unreasonable delay… [but notice] may be delayed if a law enforcement agency determines and advises the individual or entity that the notice will impede a criminal or civil investigation, or homeland or national security. Notice… must be made without unreasonable delay after the law enforcement agency determines that notification will no longer impede the investigation or jeopardize national or homeland security." "An individual or entity that maintains computerized data that includes personal information that the individual or entity does not own or license shall notify the owner or licensee of the information of any breach of the security of the system as soon as practicable following discovery."	*(Not provided for.)*

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	"Notice means: (1) Written notice to the postal address in the records of the individual or entity; (2) Telephone notice; (3) Electronic notice; or (4) Substitute notice, if the individual or the entity… demonstrates that the cost of providing notice will exceed Ten Thousand Dollars ($10,000), or that the affected class of residents to be notified exceeds five thousand (5,000) persons, or that the individual or the entity does not have sufficient contact information or consent to provide notice as described in [the immediately above] paragraphs 1, 2, or 3. Substitute notice consists of any two (2) of the following: (A) E-mail notice if the individual or the entity has e-mail addresses for the members of the affected class of residents; (B) Conspicuous posting of the notice on the Website of the individual or the entity, if the individual or the commercial entity maintains a Website; and (C) Notice to major Guam media."	
Puerto Rico P.R. Laws tit. 10, §§ 4051 – 4055 (Jun. 19, 2008)	"[An] entity that is the owner or custodian of a database that includes personal information of citizens residents of Puerto Rico must notify said citizens of any breach of the security of the system." "[An] entity that as part of their operations resells or provides access to digital data banks that at the same time contain personal information files of citizens must notify the proprietor, custodian or holder of said information."	"The notice of breach of the security of the system shall be submitted in a clear and conspicuous manner and should describe the breach of the security of the system in general terms and the type of sensitive information compromised. The notification shall also include a toll-free number and an Internet site for people to use in order to obtain information or assistance." "[As part of substitute notice, the] communication to… the media [must inform] of the situation and provid[e] information as to how to contact the entity to allow for better follow-up."

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	"Clients must be notified as expeditiously as possible, taking into consideration the need of law enforcement agencies to secure possible crime scenes and evidence as well as the application of measures needed to restore the system's security." "To notify the citizens the entity shall have the following options: (1) Written direct notice to those affected by mail or by authenticated electronic means according to [15 U.S.C. § 7001]. (2) When the cost of notifying all those potentially affected according to [the immediately above] subsection (1)… or of identifying them is excessively onerous due to the number of persons affected, to the difficulty in locating all persons or to the economic situation of the enterprise or entity; or whenever the cost exceeds one hundred thousand dollars ($100,000) or the number of persons exceeds one hundred thousand [(100,000)], the entity shall issue the notice through the following two (2) steps: (a) Prominent display of an announcement to that respect at the entities premises, on the web page of the entity, if any, and in any informative flier published and sent through mailing lists both postal and electronic, and (b) a communication to that respect to the media… When the information is of relevance to a specific professional or commercial sector, the announcement may be made through publications or programming of greater circulation oriented towards that sector."	
Virgin Islands	"[A] person or business that conducts business in the Virgin Islands, and that owns or licenses computerized data that includes personal information, shall disclose any breach of	*(Not provided for.)*

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
V.I. Code tit. 14, § 2200, §§ 2209 – 2211 (Oct. 17, 2005)	the security of the system… to any resident of the Virgin Islands whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with… any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system… [but notice] may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification… shall be made after the law enforcement agency determines that it will not compromise the investigation." "[A] person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery." "'[N]otice' may be provided by one of the following methods: (1) Written notice. (2) Electronic notice, if the notice provided is consistent with [15 U.S.C. § 7001]. (3) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed $100,000, or that the affected class of subject persons to be notified exceeds 50,000, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following: (A) E-mail notice when the person or business has an e-mail address for the subject persons.	

State & Statute	Timing & Method of Individual Notice	Content of Required Notice
	(B) Conspicuous posting of the notice on the agency's Web site page, if the person or business maintains one. (C) Notification to major territory-wide media."	

Step 3 – How and When Do I Notify Agencies?

[Back to Introduction]

State & Statute	State Agency Notice Required; Contents	State Agency Notice Instructions; Address	Consumer Reporting Agency Notice Required; Contents
Alabama Ala. Code §§ 8-38-1 – 8-38-9, 8-38-11 – 8-38-12 (Jun. 1, 2018)	"An entity subject to or regulated by federal [or state] laws, rules, regulations, procedures, or guidance on data breach notification established or enforced by the federal [or state] government [that is exempt from duplicating already-required individual notice to satisfy this law's individual notice requirement]… [must] [t]imely [provide] a copy of the [already-required individual] notice to the Attorney General when the number of individuals the entity notified exceeds 1,000." "[For all other entities,] [i]f 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… the covered entity shall provide the notice within 45 days of the covered entity's receipt of notice from a third party agent that a breach has occurred or upon the entity's determination that a breach has occurred and is reasonably likely to cause substantial harm to the individuals to whom the information relates… [but] [i]f a federal or state law enforcement agency determines that notice to individuals… 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. A law enforcement agency, by a subsequent written request, may revoke the delay as of a specified date or extend the period set forth in the original request… if further delay is necessary."	Mailing address: Office of the Attorney General P.O. Box 300152 Montgomery, AL 36130-0152 Physical address: Office of the Attorney General 501 Washington Avenue Montgomery, AL 36104	"If a covered entity discovers circumstances requiring notice… [to] 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, as defined in [15 U.S.C. §1681a], of the timing, distribution, and content of the [individual] notices."

State & Statute	State Agency Notice Required; Contents	State Agency Notice Instructions; Address	Consumer Reporting Agency Notice Required; Contents
	"[In that case] [w]ritten notice to the Attorney General shall include all of the following: (1) A synopsis of the events surrounding the breach at the time that notice is provided. (2) The approximate number of individuals in the state who were affected by the breach. (3) Any services related to the breach being offered or scheduled to be offered, without charge, by the covered entity to individuals and instructions on how to use the services. (4) The name, address, telephone number, and email address of the employee or agent of the covered entity from whom additional information may be obtained about the breach."		
Alaska Alaska Stat. §§ 45.48.010 – 45.48.090 (Jul. 1, 2009)	*(Not provided for.)*	*(N/A)*	"If an information collector is required… to notify more than 1,000 state residents of a breach, the information collector shall also notify without unreasonable delay all consumer credit reporting agencies that compile and maintain files on consumers on a nationwide basis and provide the agencies with the timing, distribution, and content of the notices to state residents." "[The consumer reporting agency notice requirement] does not apply to an information collector who is subject to the Gramm-Leach-Bliley Financial Modernization Act."

State & Statute	State Agency Notice Required; Contents	State Agency Notice Instructions; Address	Consumer Reporting Agency Notice Required; Contents
Arizona Ariz. Rev. Stat. § 18-551, § 18-552 (Aug. 3, 2018; as amended Mar 29, 2022)	"[W]ithin forty-five days after the determination… If the breach requires notification of more than one thousand individuals, notify… [t]he attorney general and the director of the Arizona department of homeland security, in writing, in a form prescribed by rule or order of the attorney general or the director of the Arizona department of homeland security or by providing the attorney general or the director of the Arizona department of homeland security with a copy of the notification provided [to affected individuals]. In the absence of a common form developed by the attorney general and the Arizona department of homeland security, nothing shall prohibit a person from submitting the same notification to the attorney general and the Arizona department of homeland security to meet the requirements of this subsection." "The notification [to the attorney general and director of the Arizona department of homeland security] may be delayed if a law enforcement agency advises the person that the notifications will impede a criminal investigation. On being informed by the law enforcement agency that the notifications no longer compromise the investigation, the person shall make the… [notification]…within forty-five days." "A person is not required to make the notification [to the attorney general] if the person, an independent third-party forensic auditor or a law enforcement agency determines after a reasonable investigation that a security system breach has not resulted in or is not reasonably likely to result in substantial economic loss to affected individuals."	Submit notice electronically via Notification of Data Breach form. Mailing and physical address: Office of the Attorney General 2005 N Central Ave Phoenix, AZ 85004-2926	"If the breach requires notification of more than one thousand individuals, notify… [t]he three largest nationwide consumer reporting agencies." "The notification [to consumer reporting agencies] may be delayed if a law enforcement agency advises the person that the notifications will impede a criminal investigation. On being informed by the law enforcement agency that the notifications no longer compromise the investigation, the person shall make the… notification[]…within forty-five days." "A person is not required to make the notification [to consumer reporting agencies] if the person, an independent third-party forensic auditor or a law enforcement agency determines after a reasonable investigation that a security system breach has not resulted in or is not reasonably likely to result in substantial economic loss to affected individuals."

State & Statute	State Agency Notice Required; Contents	State Agency Notice Instructions; Address	Consumer Reporting Agency Notice Required; Contents
Arkansas Ark. Code §§ 4-110-101 – 4-110-108 (Jul. 23, 2019)	"If a breach of the security of a system affects the personal information of more than one thousand (1,000) individuals, the person or business [that maintains computerized data that includes personal information that the person or business does not own] required to make a disclosure of the security breach [to the data owner or licensee] shall, at the same time the security breach is disclosed to an affected individual or within forty-five (45) days after the person or business determines that there is a reasonable likelihood of harm to customers, whichever occurs first, disclose the security breach to the Attorney General." "If the Attorney General submits a written request for the written determination of the breach of the security of the system, the person or business shall send a copy of the written determination of the breach of the security of the system and supporting documentation to the Attorney General no later than thirty (30) days after the date of receipt of the request." "Notification [to the Attorney General]… is not required if, after a reasonable investigation, the person or business determines that there is no reasonable likelihood of harm to customers."	Submit notice electronically via the Data Breach Reporting form. Mailing and physical address: Office of the Attorney General 323 Center Street, Suite 200 Little Rock, AR 72201	*(Not provided for.)*
California Cal. Civ. Code § 1798.80, § 1798.82, § 1798.84, § 1798.150	"A person or business that is required to issue a security breach notification… to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General."	Submit notice electronically via the Data Security Breach form. Mailing address: Office of the Attorney General P.O. Box 944255 Sacramento, CA 94244-2550	*(Not provided for.)*

State & Statute	State Agency Notice Required; Contents	State Agency Notice Instructions; Address	Consumer Reporting Agency Notice Required; Contents
(Jan. 1, 2021; § 1798.150 eff. Jan. 1, 2023)		Physical address: Office of the Attorney General 1300 "I" Street Sacramento, CA 95814-2919	
Colorado Colo. Rev. Stat. § 6-1-716 (Sep. 1, 2018)	"The covered entity that [provides individual notice]… shall provide notice of any security breach to the Colorado attorney general in the most expedient time possible and without unreasonable delay, but not later than thirty days after the date of determination that a security breach occurred, if the security breach is reasonably believed to have affected five hundred Colorado residents or more." "[Notice to the attorney general is not required if the entity] determines that the misuse of information about a Colorado resident has not occurred and is not likely to occur."	Submit notice electronically via the Data Breach Notification Form. Mailing and physical address: Office of the Attorney General Colorado Department of Law Ralph L. Carr Judicial Building 1300 Broadway, 10th Floor Denver, CO 80203	"If a covered entity is required to notify more than one thousand Colorado residents… the covered entity shall also notify, in the most expedient time possible and without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by [15 U.S.C. § 1681a(p)], of the anticipated date of the notification to the residents and the approximate number of residents who are to be notified." "[The consumer reporting agency notification requirement] does not apply to a covered entity who is subject to [15 U.S.C. §§ 6801 et seq.]"
Connecticut Conn. Gen. Stat. § 36a-701b as amended by P.A. 21-59 (Oct. 1, 2021)	"The person who owns, licenses or maintains computerized data that includes personal information, 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."	Submit notice electronically via the Data Breach Report Submission Form. Mailing and physical address: Office of the Attorney General 165 Capitol Avenue Hartford, CT 06106	*(Not provided for.)*

State & Statute	State Agency Notice Required; Contents	State Agency Notice Instructions; Address	Consumer Reporting Agency Notice Required; Contents
Delaware Del. Code tit. 6 §§ 12B-101 – 12B-104 (Apr. 14, 2018)	"If the affected number of Delaware residents to be notified exceeds 500 residents, the person… 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."	Submit notice electronically via the Security Breach Notice to the Delaware Attorney General form. Mailing and physical address: Delaware Department of Justice Carvel State Building 820 N. French Street Wilmington, DE 19801	*(Not provided for.)*
Florida Fla. Stat. § 501.171 (Oct. 1, 2019)	"A covered entity shall provide notice to the department of any breach of security affecting 500 or more individuals in this state. Such notice must be provided to the department as expeditiously as practicable, but no later than 30 days after the determination of the breach or reason to believe a breach occurred. A covered entity may receive 15 additional days to provide notice [to individuals] if good cause for delay is provided in writing to the [Department of Legal Affairs] within 30 days after determination of the breach or reason to believe a breach occurred." "The written notice to the [Department of Legal Affairs] must include: 1. A synopsis of the events surrounding the breach at the time notice is provided. 2. The number of individuals in this state who were or potentially have been affected by the breach. 3. Any services related to the breach being offered or scheduled to be offered, without charge, by the covered	Mailing address: Office of the Attorney General State of Florida PL-01 The Capitol Tallahassee, FL 32399-1050 Physical address: Consumer Protection Division Office of the Attorney General 107 West Gaines Street Collins Building, Fifth Floor Tallahassee, FL 32399	"If a covered entity discovers circumstances requiring notice… of more than 1,000 individuals at a single time, the covered entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in [15 U.S.C. s. 1681a(p)], of the timing, distribution, and content of the notices."

State & Statute	State Agency Notice Required; Contents	State Agency Notice Instructions; Address	Consumer Reporting Agency Notice Required; Contents
	entity to individuals, and instructions as to how to use such services. 4. A copy of the [individual] notice… or an explanation of the other actions taken pursuant to [the notice requirement]. 5. The name, address, telephone number, and e-mail address of the employee or agent of the covered entity from whom additional information may be obtained about the breach." "The covered entity must provide the following information to the [Department of Legal Affairs] upon its request: 1. A police report, incident report, or computer forensics report. 2. A copy of the policies in place regarding breaches. 3. Steps that have been taken to rectify the breach."		
Georgia Ga. Code § 10-1-911, § 10-1-912 (May 24, 2007)	*(Not provided for.)*	*(N/A)*	"In the event that an information broker or data collector discovers circumstances requiring notification… of more than 10,000 residents of this state at one time, the information broker or data collector shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nation-wide basis, as defined by [15 U.S.C. § 1681a], of the timing, distribution, and content of the notices."
Hawai'i Haw. Rev. Code §§ 487N-1 – 487N-3	"In the event a business provides notice to more than one thousand persons at one time… the business shall notify in writing, without unreasonable delay, the State of Hawai'i's	Mailing and physical address: Office of Consumer Protection Leiopapa A Kamehameha Building	"In the event a business provides notice to more than one thousand persons at one time… the business shall notify in writing, without unreasonable delay… all consumer reporting agencies that compile

State & Statute	State Agency Notice Required; Contents	State Agency Notice Instructions; Address	Consumer Reporting Agency Notice Required; Contents
(Jul. 1, 2008)	office of consumer protection… of the timing, distribution, and content of the notice."	235 South Beretania Street, Room 801 Honolulu, HI 96813	and maintain files on consumers on a nationwide basis, as defined in [15 U.S.C. § 1681a(p)], of the timing, distribution, and content of the notice."
Idaho Idaho Code §§ 28-51-104 – 28-51-107 (Jul. 1, 2015)	*(Not provided for.)*	*(N/A)*	*(Not provided for.)*
Illinois 815 Ill. Comp. Stat. §§ 530/1 – 530/10, §§ 530/15 – 530/20 (Jan. 1, 2020)	"[A] data collector required to issue notice… to more than 500 Illinois residents as a result of a single breach of the security system shall provide notice to the Attorney General of the breach, including: (A) A description of the nature of the breach of security or unauthorized acquisition or use. (B) The number of Illinois residents affected by such incident at the time of notification. (C) Any steps the data collector has taken or plans to take relating to the incident. Such notification must be made in the most expedient time possible and without unreasonable delay but in no event later than when the data collector provides notice to consumers… If the date of the breach is unknown at the time the notice is sent to the Attorney General, the data collector shall send the Attorney General the date of the breach as soon as possible." "[This Attorney General notice requirement] does not apply to data collectors that are covered entities or business	Submit notice via email to databreach@atg.state.il.us. Mailing and physical address: Chicago Main Office 100 West Randolph Street Chicago, IL 60601	*(Not provided for.)*

State & Statute	State Agency Notice Required; Contents	State Agency Notice Instructions; Address	Consumer Reporting Agency Notice Required; Contents
	associates and are [subject to and in compliance with the federal Health Insurance Portability and Accountability Act of 1996 and the Health Information Technology for Economic and Clinical Health Act (HITECHA), who should instead within five days of notifying the Secretary of Health and Human Services of a breach pursuant to HITECHA provide a copy of such notice to the Attorney General.]"		
Indiana Ind. Code §§ 24-4.9-1 – 24-4.9-5 (Jul. 1, 2017, as amended Mar. 18, 2022)	"If a data base owner makes a disclosure [to individuals], the data base owner shall also disclose the breach to the attorney general." "A data base owner that maintains its own disclosure procedures as part of an information privacy policy or a security policy is not required to make a separate [additional] disclosure [to the attorney general] under this [law] if the data base owner's information privacy policy or security policy is at least as stringent as the disclosure requirements described in [this law]." "A data base owner that maintains its own disclosure procedures as part of an information privacy, security policy, or compliance plan under: (1) the federal USA PATRIOT Act (P.L. 107-56); (2) Executive Order 13224; (3) [18 U.S.C. §§ 2781 et seq.]; (4) [15 U.S.C. §§ 1681 et seq.]; (5) [15 U.S.C. §§ 6801 et seq.]; or (6) the federal Health Insurance Portability and Accountability Act (HIPAA) (P.L. 104-191); is not required to make a disclosure [to the attorney general] under this [law] if the data base owner's	Complete the Indiana Data Breach Notification Form and email the completed form to databreach@atg.in.gov. Mailing and physical address: Office of Attorney General Data Privacy and Identity Theft Unit Indiana Government Center South, 5th Floor 302 W. Washington Street Indianapolis, IN 46204	"A data base owner required to make a disclosure… to more than one thousand (1,000) consumers shall also disclose to each consumer reporting agency (as defined in [15 U.S.C. § 1681a(p)]) information necessary to assist the consumer reporting agency in preventing fraud, including personal information of an Indiana resident affected by the breach of the security of a system." "A data base owner that maintains its own disclosure procedures as part of an information privacy policy or a security policy is not required to make a separate [additional] disclosure [to consumer reporting agencies] under this [law] if the data base owner's information privacy policy or security policy is at least as stringent as the disclosure requirements described in [this law]." "A data base owner that maintains its own disclosure procedures as part of an information privacy, security policy, or compliance plan under: (1) the federal USA PATRIOT Act (P.L. 107-56); (2) Executive Order 13224; (3) [18 U.S.C. §§ 2781 et seq.];

State & Statute	State Agency Notice Required; Contents	State Agency Notice Instructions; Address	Consumer Reporting Agency Notice Required; Contents
	information privacy, security policy, or compliance plan requires the data base owner to maintain reasonable procedures to protect and safeguard from unlawful use or disclosure personal information of Indiana residents that is collected or maintained by the data base owner and the data base owner complies with the data base owner's information privacy, security policy, or compliance plan." "A financial institution that complies with the disclosure requirements prescribed by the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice or the Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice, as applicable, is not required to make a disclosure [to the attorney general] under this [law]."		(4) [15 U.S.C. §§ 1681 et seq.]; (5) [15 U.S.C. §§ 6801 et seq.]; or (6) the federal Health Insurance Portability and Accountability Act (HIPAA) (P.L. 104-191); is not required to make a disclosure [to consumer reporting agencies] under this [law] if the data base owner's information privacy, security policy, or compliance plan requires the data base owner to maintain reasonable procedures to protect and safeguard from unlawful use or disclosure personal information of Indiana residents that is collected or maintained by the data base owner and the data base owner complies with the data base owner's information privacy, security policy, or compliance plan." "A financial institution that complies with the disclosure requirements prescribed by the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice or the Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice, as applicable, is not required to make a disclosure [to consumer reporting agencies] under this [law]."
Iowa Iowa Code §§ 715C.1 – 715C.2 (Jul. 1, 2018)	"[A] person who owns or licenses computerized data that includes a consumer's personal information that is used in the course of the person's business, vocation, occupation, or volunteer activities and that was subject to a breach of security requiring notification to more than five hundred residents of this state… shall give written notice of the	Submit notice via email to consumer@ag.iowa.gov. Mailing and physical address: Consumer Protection Division Security Breach Notifications	*(Not provided for.)*

State & Statute	State Agency Notice Required; Contents	State Agency Notice Instructions; Address	Consumer Reporting Agency Notice Required; Contents
	breach of security to the director of the consumer protection division of the office of the attorney general within five business days after giving notice of the breach of security to any consumer." "[The director of the consumer protection division notice requirement] does not apply to any of the following: a. A person who complies with notification requirements or breach of security procedures that provide greater protection to personal information and at least as thorough disclosure requirements than that provided by this [law] pursuant to the rules, regulations, procedures, guidance, or guidelines established by the person's primary or functional federal regulator. b. A person who complies with a state or federal law that provides greater protection to personal information and at least as thorough disclosure requirements for breach of security or personal information than that provided by this [law]. c. A person who is subject to and complies with regulations promulgated pursuant to [15 U.S.C. §§ 6801 – 6809]. d. A person who is subject to and complies with regulations promulgated pursuant to [42 U.S.C. §§ 1320d – 1320d(9), and [42 U.S.C. §§ 17921 – 17954]."	Office of the Attorney General of Iowa 1305 E. Walnut Street Des Moines, IA 50319-0106	
Kansas Kan. Stat. §§ 50-7a01 – 50-7a02 (Jul. 1, 2006)	*(Not provided for.)*	*(N/A)*	"In the event that a person discovers circumstances requiring notification… of more than 1,000 consumers at one time, the person shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by 15

State & Statute	State Agency Notice Required; Contents	State Agency Notice Instructions; Address	Consumer Reporting Agency Notice Required; Contents
			U.S.C. § 1681a(p), of the timing, distribution and content of the notices."
Kentucky Ky. Rev. Stat. § 365.732 (Jul. 15, 2014)	*(Not provided for.)*	*(N/A)*	"If a person discovers circumstances requiring notification… of more than one thousand (1,000) persons at one (1) time, the person shall also notify, without unreasonable delay, all consumer reporting agencies and credit bureaus that compile and maintain files on consumers on a nationwide basis, as defined by [15 U.S.C. § 1681a], of the timing, distribution, and content of the notices."
Louisiana La. Rev. Stat. §§ 51:3071 – 51:3077 (Aug. 1, 2018) La. Admin. Code tit. 16, pt. III, § 701 (Mar. 20, 2007)	"When notice to Louisiana citizens is required pursuant to [La. Rev. Stat. § 51:3074], the person… shall provide written notice detailing the breach of the security of the system to the Consumer Protection Section of the Attorney General's Office. Notice shall include the names of all Louisiana citizens affected by the breach." "Notice to the attorney general shall be timely if received within 10 days of distribution of notice to Louisiana citizens."	Submit written notification via postal mail. Mailing and physical address: Louisiana Department of Justice Office of the Attorney General Consumer Protection Section 1885 N. Third Street Baton Rouge, LA 70802	*(Not provided for.)*
Maine Me. Stat. tit. 10, §§ 1346 – 1350-A (Sep. 19, 2019)	"When notice of a breach of the security of the system is required [to affected individuals], the person shall notify the appropriate state regulators within the Department of Professional and Financial Regulation, or if the person is not regulated by the department, the Attorney General."	Contact information for state regulators within the Department of Professional and Financial Regulation available on the Department's website.	"If a person discovers a breach of the security of the system that requires notification to more than 1,000 persons at a single time, the person shall… notify, without unreasonable delay, consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in [15 U.S.C. § 1681a(p)]. Notification must include the date

State & Statute	State Agency Notice Required; Contents	State Agency Notice Instructions; Address	Consumer Reporting Agency Notice Required; Contents
		Submit notice to the Attorney General electronically via the Maine Security Breach Reporting Form. Attorney General mailing and physical address: Office of the Maine Attorney General 6 State House Station Augusta, ME 04333	of the breach, an estimate of the number of persons affected by the breach, if known, and the actual or anticipated date that persons were or will be notified of the breach."
Maryland Md. Com. Law §§ 14-3501 – 14-3508 (Oct. 1, 2022)	"Prior to giving the [individual] notification…a business shall provide notice of a breach of the security of a system to the Office of the Attorney General." "The notice required… shall include, at a minimum: (i) The number of affected individuals residing in the State; (ii) A description of the breach of the security of a system, including when and how it occurred; (iii) Any steps the business has taken or plans to take relating to the breach of the security of a system; and (iv) The form of notice that will be sent to affected individuals and a sample notice. "[Notice to the Office of the Attorney General] may be delayed… [i]If a law enforcement agency determines that the notification will impede a criminal investigation or jeopardize homeland or national security… [or in order] [t]o determine the scope of the breach of the security of a system, identify the individuals affected, or restore the integrity of the system."	Submit notice via email to idtheft@oag.state.md.us. Mailing and physical address: Office of the Attorney General Attn: Security Breach Notification 200 St. Paul Place Baltimore, MD 21202 Fax address: Attn: Security Breach Notification (410) 576-6566	"If a business is required… to give notice of a breach of the security of a system to 1,000 or more individuals, the business also shall notify, without unreasonable delay, each consumer reporting agency that compiles and maintains files on consumers on a nationwide basis, as defined by 15 U.S.C. § 1681a(p), of the timing, distribution, and content of the notices."

State & Statute	State Agency Notice Required; Contents	State Agency Notice Instructions; Address	Consumer Reporting Agency Notice Required; Contents
Massachusetts Mass. Gen. Laws §§ 93H-1 – 93H-6 (Apr. 10, 2019)	"A person… that owns or licenses data that includes personal information about a resident of the commonwealth, shall provide notice, as soon as practicable and without unreasonable delay, when such person [provides notice to affected individuals]… to the attorney general… [and to] the director of consumer affairs and business regulation." "The notice to be provided to the attorney general and said director, and… state agencies if any, shall include, but not be limited to: (i) the nature of the breach of security or unauthorized acquisition or use; (ii) the number of residents of the commonwealth affected by such incident at the time of notification; (iii) the name and address of the person or agency that experienced the breach of security; (iv) name and title of the person or agency reporting the breach of security, and their relationship to the person or agency that experienced the breach of security; (v) the type of person or agency reporting the breach of security; (vi) the person responsible for the breach of security, if known; (vii) the type of personal information compromised, including, but not limited to, social security number, driver's license number, financial account number, credit or debit card number or other data; (viii) whether the person or agency maintains a written information security program; and (ix) any steps the person or agency has taken or plans to take relating to the incident, including updating the written information security program."	Submit notice to the Attorney General electronically via the Reporting data breaches to the Attorney General's Office online portal. Submit notice to the Director of Consumer Affairs and Business Regulation electronically via a separate Data Breach Notification Submission form. Attorney General mailing and physical address: Massachusetts Office of the Attorney General Data Privacy and Security Division Attn: Data Breach Notification One Ashburton Place Boston, MA 02108 Director of Consumer Affairs and Business Regulation mailing and physical address: Office of Consumer Affairs and Business Regulation Attn: Undersecretary Edward A. Palleschi 501 Boylston Street Suite 5100 Boston, MA 02116	"Upon receipt of… notice, the director of consumer affairs and business regulation shall identify any relevant consumer reporting agency…, as deemed appropriate by said director, and forward the names of the identified consumer reporting agencies… to the notifying person… [who] shall, as soon as practicable and without unreasonable delay, also provide notice… to [those] consumer reporting agencies." "The notice to be provided to… consumer reporting agencies… shall include, but not be limited to [the same nine items (i) – (ix) required for the notice to the attorney general and director of consumer affairs and business regulation]."

Step 3 - How and When Do I Notify Agencies?
[Back to Introduction]

State & Statute	State Agency Notice Required; Contents	State Agency Notice Instructions; Address	Consumer Reporting Agency Notice Required; Contents
	"A person who experienced a breach of security shall file a report with the attorney general and the director of consumer affairs and business regulation certifying their credit monitoring services comply with [Mass. Gen. Laws § 93H-3A]." "The person… that experienced the breach of security shall provide a sample copy of the notice it sent to consumers to the attorney general and the office of consumer affairs and business regulation… [which may] not be delayed on grounds that the total number of residents affected is not yet ascertained. In such case, and where otherwise necessary to update or correct the information required, a person… shall provide additional notice as soon as practicable and without unreasonable delay upon learning such additional information." "Upon receipt of… notice, the director of consumer affairs and business regulation shall identify any relevant… state agency, as deemed appropriate by said director, and forward the names of the identified… state agencies to the notifying person or agency. Such person… shall, as soon as practicable and without unreasonable delay, also provide notice… [to those] state agencies." "The notice to be provided to… [such] state agencies… shall include, but not be limited to [the same nine items (i) – (ix) required for the notice to the attorney general and director of consumer affairs and business regulation]."		

State & Statute	State Agency Notice Required; Contents	State Agency Notice Instructions; Address	Consumer Reporting Agency Notice Required; Contents
Michigan Mich. Comp. Laws §§ 445.61 – 445.64, § 445.72, § 445.72b (Jan. 1, 2020)	*(Not provided for.)*	*(N/A)*	"[A]fter a person… provides a notice [to affected individuals], the person… shall notify each consumer reporting agency that compiles and maintains files on consumers on a nationwide basis, as defined in [15 U.S.C. § 1681a(p)], of the security breach without unreasonable delay… [including in the notice] the number of notices that the person… provided to residents of this state and the timing of those notices." "[The consumer reporting agency notice requirement] does not apply if either of the following is met: (a) The person… is required… to provide notice of a security breach to 1,000 or fewer residents of this state. (b) The person… is subject to [15 U.S.C. §§ 6801 – 6809].
Minnesota Minn. Stat. § 325E.61 (Jul. 1, 2006)	*(Not provided for.)*	*(N/A)*	If a person discovers circumstances requiring [individual] notification… of more than 500 persons at one time, the person shall also notify, within 48 hours, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by [15 U.S.C. § 1681a], of the timing, distribution, and content of the notices.
Mississippi Miss. Code § 75-24-29 (Jul. 1, 2021)	*(Not provided for.)*	*(N/A)*	*(Not provided for.)*

State & Statute	State Agency Notice Required; Contents	State Agency Notice Instructions; Address	Consumer Reporting Agency Notice Required; Contents
Missouri Mo. Rev. Stat. § 407.1500 (Aug. 28, 2009)	"In the event a person provides notice to more than one thousand consumers at one time… the person shall notify, without unreasonable delay, the attorney general's office… of the timing, distribution, and content of the notice."	Mailing address: Missouri Attorney General's Office P.O. Box 899 Jefferson City, MO 65102 Physical address: Missouri Attorney General's Office Supreme Court Building 207 W High Street Jefferson City, MO 65101	"In the event a person provides notice to more than one thousand consumers at one time… the person shall notify, without unreasonable delay… all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in [15 U.S.C. § 1681a(p)], of the timing, distribution, and content of the notice."
Montana Mont. Code § 30-14-1702, §§ 30-14-1704 – 30-14-1705 (Oct. 1, 2015)	"[A] person or business that is required to issue a notification [to an individual] shall simultaneously submit an electronic copy of the notification and a statement providing the date and method of distribution of the notification to the attorney general's consumer protection office, excluding any information that personally identifies any individual who is entitled to receive notification. If a notification is made to more than one individual, a single copy of the notification must be submitted that indicates the number of individuals in the state who received notification."	Submit notice via email to ocpdatabreach@mt.gov. Mailing address: Montana Department of Justice Office of Consumer Protection P.O. Box 200151 Helena, MT 59620-0151 Physical address: Montana Department of Justice Office of Consumer Protection 555 Fuller Avenue Helena, MT 59601-3394	"If a business discloses a security breach to any individual pursuant to this section and gives a notice to the individual that suggests, indicates, or implies to the individual that the individual may obtain a copy of the file on the individual from a consumer credit reporting agency, the business shall coordinate with the consumer reporting agency as to the timing, content, and distribution of the notice to the individual. The coordination may not unreasonably delay the notice to the affected individuals."
Nebraska Neb. Rev. Stat. §§ 87-801 – 87-807 (Jul. 18, 2018)	"If notice of a breach of security of the system is required [to individuals]… the individual or commercial entity shall also, not later than the time when notice is provided to the	Submit notice electronically via the Data Breach Notification form, or print and complete a hard copy form and send the	*(Not provided for.)*

State & Statute	State Agency Notice Required; Contents	State Agency Notice Instructions; Address	Consumer Reporting Agency Notice Required; Contents
	Nebraska resident, provide notice of the breach of security of the system to the Attorney General."	completed form via postal mail to the Attorney General. Mailing and physical address: Office of the Attorney General Consumer Protection Division 2115 State Capitol Lincoln, NE 68509	
Nevada Nev. Rev. Stat. §§ 603A.010 – 603A.100, §§ 603A.215 – 603A.290 (Oct. 1, 2021)	*(Not provided for.)*	*(N/A)*	"If a data collector determines that notification is required to be given… to more than 1,000 persons at any one time, the data collector shall also notify, without unreasonable delay, any consumer reporting agency that compiles and maintains files on consumers on a nationwide basis, as that term is defined in 15 U.S.C. § 1681a(p) of the time the notification is distributed and the content of the notification."
New Hampshire N.H. Rev. Stat. §§ 359-C:19 – 359-C:21 (Jan. 1, 2007)	"[A] person engaged in trade or commerce that is subject to [N.H. Rev. Stat. § 358-A:3], shall… notify the regulator which has primary regulatory authority over such trade or commerce. All other persons shall notify the New Hampshire attorney general's office." "The notice shall include the anticipated date of the notice to the individuals and the approximate number of individuals in this state who will be notified… The disclosure shall be made to affected individuals as quickly as possible, after the determination [that misuse of the information has occurred or is reasonably likely to occur]."	Contact information for state regulators available on the state government's website. Mailing and physical address: N.H. Department of Justice Office of the Attorney General 33 Capitol Street Concord, NH 03301	"If a person is required to notify more than 1,000 consumers of a breach of security… the person shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by [15 U.S.C. § 1681a(p)], of the anticipated date of the notification to the consumers, the approximate number of consumers who will be notified, and the content of the notice." "[The consumer reporting agency notice requirement] shall not apply to a person who is subject to [15 U.S.C. §§ 6801 et seq.]"

State & Statute	State Agency Notice Required; Contents	State Agency Notice Instructions; Address	Consumer Reporting Agency Notice Required; Contents
New Jersey N.J. Stat. § 56:8-161, § 56:8-163, §§ 56:8-165 – 56:8-166 (Sep. 1, 2019)	"[A] business or public entity required… to disclose a breach of security of a customer's personal information [to affected individuals] shall, in advance of the disclosure to the customer, report the breach of security and any information pertaining to the breach to the Division of State Police in the Department of Law and Public Safety for investigation or handling, which may include dissemination or referral to other appropriate law enforcement entities."	Submit notice electronically via the Data Breach Report Form. Mailing address: New Jersey State Police P.O. Box 7068 West Trenton, NJ 08628 Physical address: New Jersey State Police Public Health, Environmental and Agricultural Laboratory Building 3 Schwarzkopf Drive Ewing Township, NJ 08628	"[I]n the event that a business or public entity discovers circumstances requiring notification… of more than 1,000 persons at one time, the business or public entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile or maintain files on consumers on a nationwide basis, as defined by [15 U.S.C. 1681a(p)], of the timing, distribution and content of the notices."
New Mexico N.M. Stat. §§ 57-12C-1 – 57-12C-2, §§ 57-12C-6 – 57-12C-11 (Jun. 16, 2017)	"A person that is required to issue notification of a security breach… to more than one thousand New Mexico residents as a result of a single security breach shall notify the office of the attorney general… of the security breach in the most expedient time possible, and no later than forty-five calendar days… following discovery of the security breach." "[Notice to the office of the attorney general] may be delayed: A. if a law enforcement agency determines that the notification will impede a criminal investigation; or B. as necessary to determine the scope of the security breach and restore the integrity, security and confidentiality of the data system."	Mailing and physical address: Office of the Attorney General 408 Galisteo Street Villagra Building Santa Fe, NM 87501	"A person that is required to issue notification of a security breach… to more than one thousand New Mexico residents as a result of a single security breach shall notify the… major consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in [15 U.S.C. § 1681a(p)], of the security breach in the most expedient time possible, and no later than forty-five calendar days [following discovery of the security breach]." "[Notice to consumer reporting agencies] may be delayed: A. if a law enforcement agency determines that the notification will impede a criminal investigation; or

State & Statute	State Agency Notice Required; Contents	State Agency Notice Instructions; Address	Consumer Reporting Agency Notice Required; Contents
	"[Notification shall include] the number of New Mexico residents that received [individual] notification… and shall provide a copy of the notification that was sent to affected residents."		B. as necessary to determine the scope of the security breach and restore the integrity, security and confidentiality of the data system."
New York N.Y. Gen. Bus. Law § 899-AA (Oct. 23, 2019)	"In the event that any New York residents are to be notified, the person or business shall notify the state attorney general, the department of state and the division of state police as to the timing, content and distribution of the notices and approximate number of affected persons and shall provide a copy of the template of the notice sent to affected persons. Such notice shall be made without delaying notice to affected New York residents." "[If the person or business determines the circumstances of the breach incident do not require individual notice, and] [i]f the incident affects over five hundred residents of New York, the person or business shall provide the written determination to the state attorney general within ten days after the determination."	Submit notice simultaneously to the state attorney general, department of state, and division of state police, or submit written determination to the state attorney general electronically via the online Data Breach Reporting Form. Mailing and physical addresses: Office of the Attorney General The Capitol Albany, NY 12224-0341 Department of State One Commerce Plaza, 99 Washington Avenue Albany, NY 12210 Division of State Police Concourse, Empire State Plaza Albany, NY 12242	"In the event that more than five thousand New York residents are to be notified at one time, the person or business shall also notify consumer reporting agencies as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York residents." "'Consumer reporting agency' shall mean any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports."
North Carolina	"In the event a business provides notice to an affected person… the business shall notify without unreasonable delay the Consumer Protection Division of the Attorney	Submit notice electronically via the Security Breach Form.	"In the event a business provides notice to more than 1,000 persons at one time… the business shall notify, without unreasonable delay… all consumer

State & Statute	State Agency Notice Required; Contents	State Agency Notice Instructions; Address	Consumer Reporting Agency Notice Required; Contents
N.C. Gen. Stat. § 75-60, § 75-61, § 75-65 (Jan. 1, 2016)	General's Office of the nature of the breach, the number of consumers affected by the breach, steps taken to investigate the breach, steps taken to prevent a similar breach in the future, and information regarding the timing, distribution, and content of the notice." "In the event a business provides notice to more than 1,000 persons at one time… the business shall notify, without unreasonable delay, the Consumer Protection Division of the Attorney General's Office… of the timing, distribution, and content of the notice." "'Consumer'… [means] [a]n individual."	Mailing and physical address: Consumer Protection Division of the Attorney General's Office Department of Justice 9001 Mail Service Center Raleigh, NC 27699-9001	reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. § 1681a(p), of the timing, distribution, and content of the notice."
North Dakota N.D. Cent. Code §§ 51-30-01 – 51-30-07 (Aug. 1, 2015)	"[A] person that experiences a breach of the security system… shall disclose to the attorney general by mail or electronic mail any breach of the security system which exceeds two hundred fifty individuals. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with… any measures necessary to determine the scope of the breach and to restore the integrity of the data system… [but notice to the attorney general] may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification… must be made after the law enforcement agency determines that the notification will not compromise the investigation."	Submit notice via email to ndag@nd.gov. Mailing and physical address: Office of Attorney General 600 E. Boulevard Avenue, Dept. 125 Bismarck, ND 58505-0040	*(Not provided for.)*
Ohio	*(Not provided for.)*	*(N/A)*	"If a person discovers circumstances that require disclosure… to more than one thousand residents of this state involved in a single occurrence of a breach

State & Statute	State Agency Notice Required; Contents	State Agency Notice Instructions; Address	Consumer Reporting Agency Notice Required; Contents
Ohio Rev. Code §§ 1349.19 – 1349.192 (Mar. 30, 2007)			of the security of the system, the person shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution, and content of the disclosure given by the person to the residents of this state." "[The person may not] delay any disclosure or notification [to consumers or by data custodians]… in order to make the notification [to consumer reporting agencies]." "'Consumer reporting agency that compiles and maintains files on consumers on a nationwide basis' means a consumer reporting agency that regularly engages in the practice of assembling or evaluating, and maintaining, for the purpose of furnishing consumer reports to third parties bearing on a consumer's creditworthiness, credit standing, or credit capacity, each of the following regarding consumers residing nationwide: (a) Public record information; (b) Credit account information from persons who furnish that information regularly and in the ordinary course of business."
Oklahoma Okla. Stat. tit. 24, §§ 161 – 166 (Nov. 1, 2008)	*(Not provided for.)*	*(N/A)*	*(Not provided for.)*

State & Statute	State Agency Notice Required; Contents	State Agency Notice Instructions; Address	Consumer Reporting Agency Notice Required; Contents
Oregon Or. Rev. Stat. §§ 646A.600 – 646A.604, 646A.624 – 646A.628 (Jan. 1, 2020)	"[T]he covered entity shall give notice of the breach of security to… [t]he Attorney General, either in writing or electronically, if the number of consumers to whom the covered entity must send the [individual] notice… exceeds 250." "A vendor shall notify the Attorney General in writing or electronically if the vendor was subject to a breach of security that involved the personal information of more than 250 consumers or a number of consumers that the vendor could not determine… [but this requirement] does not apply… if the covered entity [that the vendor contracts with, or that the vendor's vendor has a contract with]… has notified the Attorney General." "[A] person, a covered entity or a vendor shall provide to the Attorney General within a reasonable time at least one copy of any notice the person, the covered entity or the vendor sends to consumers or to the person's, the covered entity's or the vendor's primary or functional regulator in compliance with this [law] or with other state or federal laws or regulations that apply to the person, the covered entity or the vendor as a consequence of a breach of security, if the breach of security affects more than 250 consumers."	Submit notice electronically via the Report Data Breaches form. Mailing and physical address: Oregon Department of Justice Office of the Attorney General 1162 Court Street NE Salem, OR 97301-4096	"If a covered entity discovers or receives notice of a breach of security that affects more than 1,000 consumers, the covered entity shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain reports on consumers on a nationwide basis of the timing, distribution and content of the notice the covered entity gave to affected consumers and shall include in the notice any police report number assigned to the breach of security." "A covered entity may not delay notifying affected consumers of a breach of security in order to notify consumer reporting agencies."
Pennsylvania 73 Pa. Cons. Stat. §§ 2301 – 2330 (May 2, 2023)	*(Not provided for.)*	*(N/A)*	"When an entity provides notification… to more than 1,000 persons at one time, the entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in [15

State & Statute	State Agency Notice Required; Contents	State Agency Notice Instructions; Address	Consumer Reporting Agency Notice Required; Contents
			U.S.C. § 1681a], of the timing, distribution and number of notices."
Rhode Island R.I. Gen. Laws § 11-49.3-1, §§ 11-49.3-3 – 11-49.3-6 (Jul. 2, 2016)	"In the event that more than five hundred (500) Rhode Island residents are to be notified, the… person shall notify the attorney general… as to the timing, content, and distribution of the notices and the approximate number of affected individuals. Notification to the attorney general… shall be made without delaying notice to affected Rhode Island residents."	Mailing and physical address: Office of the Attorney General 150 South Main Street Providence, RI 02903	"In the event that more than five hundred (500) Rhode Island residents are to be notified, the… person shall notify… the major credit reporting agencies as to the timing, content, and distribution of the notices and the approximate number of affected individuals. Notification to… the major credit reporting agencies shall be made without delaying notice to affected Rhode Island residents."
South Carolina S.C. Code § 39-1-90 (Apr. 23, 2013)	"If a business provides notice to more than one thousand persons at one time… the business shall notify, without unreasonable delay, the Consumer Protection Division of the Department of Consumer Affairs… of the timing, distribution, and content of the notice."	Submit notice via email to scdca@scconsumer.gov or via postal mail. Mailing address: Department of Consumer Affairs Legal Division P.O. Box 5757 Columbia, SC 29250 Physical address: Department of Consumer Affairs Legal Division 293 Greystone Boulevard, Suite 400 Columbia, SC 29210	"If a business provides notice to more than one thousand persons at one time… the business shall notify, without unreasonable delay… all consumer reporting agencies that compile and maintain files on a nationwide basis, as defined in [15 U.S.C. § 1681a(p)], of the timing, distribution, and content of the notice."

State & Statute	State Agency Notice Required; Contents	State Agency Notice Instructions; Address	Consumer Reporting Agency Notice Required; Contents
South Dakota S.D. Cod. Laws §§ 22-40-19 – 22-40-26 (Jul. 1, 2018)	"[An] information holder that experiences a breach of system security… shall disclose to the attorney general by mail or electronic mail any breach of system security that exceeds two hundred fifty residents of this state."	Submit notice via email to consumerhelp@state.sd.us. Mailing and physical address: Office of the Attorney General 1302 E. Highway 14, Suite 1 Pierre, SD 57501-8501	"If an information holder discovers circumstances that require [individual] notification… the information holder shall also notify, without unreasonable delay, all consumer reporting agencies, as defined under 15 U.S.C. § 1681a in effect as of January 1, 2018, and any other credit bureau or agency that compiles and maintains files on consumers on a nationwide basis, of the timing, distribution, and content of the notice."
Tennessee Tenn. Code § 47-18-2107 (Apr. 4, 2017)	*(Not provided for.)*	*(N/A)*	"If an information holder discovers circumstances requiring notification… of more than one thousand (1,000) persons at one (1) time, the information holder must also notify, without unreasonable delay, all consumer reporting agencies, as defined by 15 U.S.C. § 1681a, and credit bureaus that compile and maintain files on consumers on a nationwide basis, of the timing, distribution, and content of the notices."
Texas Tex. Bus. & Com. Code § 521.002, § 521.053, § 521.151 (As amended by SB 768, effective Sep. 1, 2023)	"A person who is required to disclose or provide notification of a breach of system security… shall notify the attorney general of that breach as soon as practicable and not later than the 30th day after the date on which the person determines that the breach occurred if the breach involves at least 250 residents of this state. The notification… must include: (1) a detailed description of the nature and circumstances of the breach or the use of sensitive personal information acquired as a result of the breach;	Submit notice electronically via the Data Security Breach Report form.	"If a person is required… to notify at one time more than 10,000 persons of a breach of system security, the person shall also notify each consumer reporting agency, as defined by [15 U.S.C. § 1681a], that maintains files on consumers on a nationwide basis, of the timing, distribution, and content of the notices… without unreasonable delay."

State & Statute	State Agency Notice Required; Contents	State Agency Notice Instructions; Address	Consumer Reporting Agency Notice Required; Contents
	(2) the number of residents of this state affected by the breach at the time of notification; (3) the number of affected residents that have been sent a disclosure of the breach by mail or other direct method of communication at the time of notification; (4) the measures taken by the person regarding the breach; (5) any measures the person intends to take regarding the breach after the notification [to the attorney general]; and (6) information regarding whether law enforcement is engaged in investigating the breach."		
Utah Utah Code §§ 13-44-101 – 13-44-103, § 13-44-202, § 13-44-301 (May 3, 2023)	"If… the misuse of personal information relating to 500 or more Utah residents… has occurred or is reasonably likely to occur, the person shall… provide notification to… the Office of the Attorney General; and … the Utah Cyber Center." "Information submitted to the Utah Cyber Center… regarding a breach… may include information regarding the type of breach, the attack vector, attacker, indicators of compromise, and other details of the breach that are requested by the Utah Cyber Center." "A person required to provide notification [to the Attorney General and Utah Cyber Center]… shall [do so]… in the most expedient time possible without unreasonable delay: (a) considering legitimate investigative needs of law enforcement…, (b) after determining the scope of the breach of system security; and (c) after restoring the reasonable integrity of the system."	Attorney General mailing address: Office of the Attorney General PO Box 142320 Salt Lake City, UT 84114-2320 Attorney General physical address: Office of the Attorney General 350 North State Street Suite 230 Salt Lake City, UT 84114	"If… the misuse of personal information relating to 1,000 or more Utah residents… has occurred or is reasonably likely to occur, the person shall… provide notification to each consumer reporting agency that compiles and maintains files on consumers on a nationwide basis, as defined in [15 U.S.C. § 1681a]."

Step 3 - How and When Do I Notify Agencies?
[Back to Introduction]

State & Statute	State Agency Notice Required; Contents	State Agency Notice Instructions; Address	Consumer Reporting Agency Notice Required; Contents
Vermont Vt. Stat. tit. 9, § 2430, § 2435 (Jul. 1, 2020)	"A data collector or other entity regulated by the Department of Financial Regulation under [Vt. Stat. tit. 8, §§ 1 et seq. or tit. 9, §§ 1 et seq.] shall provide notice of a breach to [such] Department. All other data collectors or other entities… shall provide notice of a breach to the Attorney General." "[A] data collector who, prior to the date of the breach, on a form and in a manner prescribed by the Attorney General, had sworn in writing to the Attorney General that it maintains written policies and procedures to maintain the security of personally identifiable information or login credentials and respond to a breach in a manner consistent with Vermont law shall notify the Attorney General of the date of the security breach and the date of discovery of the breach and shall provide a description of the breach prior to providing notice of the breach to consumers." "When the data collector provides [individual] notice of the breach… the data collector shall notify the Attorney General or the Department, as applicable, of the number of Vermont consumers affected, if known to the data collector, and shall provide a copy of the [individual] notice provided to consumers." "The data collector shall notify the Attorney General or the Department, as applicable, of the date of the security breach and the date of discovery of the breach and shall provide a preliminary description of the breach within 14 business days, consistent with [delayed individual notice based on] the legitimate needs of the law enforcement agency… of the data collector's discovery of the security	Submit notice to the Attorney General via email to ago.securitybreach@vermont.gov. Submit notice to the Department of Financial Regulation via postal mail. Attorney General mailing and physical address: Vermont Attorney General's Office 109 State Street Montpelier, VT 05609 Department of Financial Regulation mailing and physical address: Department of Financial Regulation General Counsel 89 Main Street Montpelier, VT 05620-3101	"In the event a data collector provides notice to more than 1,000 consumers at one time… the data collector shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. § 1681a(p), of the timing, distribution, and content of the notice." "[The consumer reporting agency notice requirement] shall not apply to a person who is licensed or registered under [Vt. Stat. tit. 8, §§ 1 et seq.] by the Department of Financial Regulation."

State & Statute	State Agency Notice Required; Contents	State Agency Notice Instructions; Address	Consumer Reporting Agency Notice Required; Contents
	breach or when the data collector provides notice to consumers… whichever is sooner." "If the date of the breach is unknown at the time notice is sent to the Attorney General or to the Department, the data collector shall send the Attorney General or the Department the date of the breach as soon as it is known." "[But] [i]f a security breach is limited to an unauthorized acquisition of login credentials, a data collector is only required to provide notice of the security breach to the Attorney General or Department of Financial Regulation, as applicable, if the login credentials were acquired directly from the data collector or its agent."		
Virginia Va. Code § 18.2-186.6 (Jul. 1, 2020)	"[A]n individual or entity that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system… to the Office of the Attorney General… without unreasonable delay. Notice… may be reasonably delayed to allow the individual or entity to determine the scope of the breach of the security of the system and restore the reasonable integrity of the system… [or] if, after the individual or entity notifies a law-enforcement agency, the law-enforcement agency determines and advises the individual or entity that the notice will impede a criminal or civil investigation, or homeland or national security. [In that case,] [n]otice shall be made without unreasonable delay after the law-enforcement agency determines that the notification will no longer impede the investigation or jeopardize national or homeland security."	Submit notice via postal mail to the Computer Crime Section of the Attorney General's Office. Mailing and physical address: Office of the Attorney General Computer Crime Section 202 North 9th Street Richmond, VA 23219	"In the event an individual or entity provides notice to more than 1,000 persons at one time… the individual or entity shall notify, without unreasonable delay… all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. § 1681a(p), of the timing, distribution, and content of the notice."

State & Statute	State Agency Notice Required; Contents	State Agency Notice Instructions; Address	Consumer Reporting Agency Notice Required; Contents
	"In the event an individual or entity provides notice to more than 1,000 persons at one time… the individual or entity shall notify, without unreasonable delay, the Office of the Attorney General… of the timing, distribution, and content of the notice." "A [data] processor shall adhere to the instructions of a [data] controller and shall assist the controller in meeting its obligations… includ[ing,]… taking into account the nature of processing and the information available to the processor, by assisting the controller in meeting the controller's obligations in relation to… the notification of a breach of security of the system of the processor."		
Washington Wash. Rev. Code §§ 19.255.005 – 19.255.040 (Mar. 1, 2020)	"Covered entities [under 42 U.S.C. §§ 1320d et seq.] shall notify the attorney general [of the breach]… [in accordance] with the timeliness of notification requirements of section 13402 of the federal health information technology for economic and clinical health act, P.L. 111-5 as it existed on July 24, 2015." "[Otherwise, a] person or business that is required to issue a notification… to more than five hundred Washington residents as a result of a single breach shall notify the attorney general of the breach no more than thirty days after the breach was discovered." "The notice to the attorney general shall include the following information: (i) The number of Washington consumers affected by the breach, or an estimate if the exact number is not known;	Submit notice electronically via the Data Breach Notification Form. Mailing address: Office of the Attorney General 1125 Washington Street SE P.O. Box 40100 Olympia, WA 98504-0100 Physical address: Office of the Attorney General 1125 Washington Street S.E. Olympia, WA 98504-0100	*(Not provided for.)*

State & Statute	State Agency Notice Required; Contents	State Agency Notice Instructions; Address	Consumer Reporting Agency Notice Required; Contents
	(ii) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach; (iii) A time frame of exposure, if known, including the date of the breach and the date of the discovery of the breach; (iv) A summary of steps taken to contain the breach; and (v) A single sample copy of the [individual] security breach notification, excluding any personally identifiable information." "The notice to the attorney general must be updated if any of the information [required to be included in the notice] is unknown at the time notice is due."		
West Virginia W. Va. Code §§ 46A-2A-101 – 46A-2A-105 (Jun. 7, 2008)	*(Not provided for.)*	*(N/A)*	"If an entity is required to notify more than one thousand persons of a breach of security… the entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on a nationwide basis, as defined by 15 U.S.C. §1681a(p), of the timing, distribution and content of the notices." "[The consumer reporting agency notice requirement] shall not apply to an entity who is subject to [15 U.S.C. §§ 6801 et seq.]"
Wisconsin Wis. Stat. §§ 134.98 – 134.99 (Mar. 28, 2008)	*(Not provided for.)*	*(N/A)*	"If, as the result of a single incident, an entity is required… to notify 1,000 or more individuals that personal information pertaining to the individuals has been acquired, the entity shall without unreasonable delay notify all consumer reporting

State & Statute	State Agency Notice Required; Contents	State Agency Notice Instructions; Address	Consumer Reporting Agency Notice Required; Contents
			agencies that compile and maintain files on consumers on a nationwide basis, as defined in [15 U.S.C. § 1681a(p)], of the timing, distribution, and content of the notices sent to the individuals." "A law enforcement agency may, in order to protect an investigation or homeland security, ask an entity not to provide a notice that is otherwise required [to consumer reporting agencies]… for any period of time and the notification process… shall begin at the end of that time period… [and] if an entity receives such a request, the entity may not provide notice of or publicize an unauthorized acquisition of personal information, except as authorized by the law enforcement agency that made the request."
Wyoming Wyo. Stat. §§ 40-12-501 – 40-12-502 (Jul. 1, 2015) Wyo. Stat. § 6-3-901(b)(iii)–(xiv) (Jul. 1, 2015)	*(Not provided for.)*	*(N/A)*	*(Not provided for.)*
District of Columbia D.C. Code §§ 28-3851 – 28-3853 (Jun. 17, 2020)	"[T]he person or entity required to give notice shall promptly provide written notice of the breach of the security of the system to the Office of the Attorney General for the District of Columbia if the breach affects 50 or more District residents. This notice shall be made in the most	Submit notice via email to databreach@dc.gov. Mailing and physical address: Office of the Attorney General	"If [a] person or entity is required… to notify more than 1,000 persons of a breach of security… the person shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis,

Step 3 - How and When Do I Notify Agencies?
[Back to Introduction]

State & Statute	State Agency Notice Required; Contents	State Agency Notice Instructions; Address	Consumer Reporting Agency Notice Required; Contents
	expedient manner possible, without unreasonable delay, and in no event later than when [individual] notice is provided… [but this notice] may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation but shall be made as soon as possible after the law enforcement agency determines that the notification will not compromise the investigation." "The written notice shall include: (1) The name and contact information of the person or entity reporting the breach; (2) The name and contact information of the person or entity that experienced the breach; (3) The nature of the breach of the security of the system, including the name of the person or entity that experienced the breach; (4) The types of personal information compromised by the breach; (5) The number of District residents affected by the breach; (6) The cause of the breach, including the relationship between the person or entity that experienced the breach and the person responsible for the breach, if known; (7) The remedial action taken by the person or entity to include steps taken to assist District residents affected by the breach; (8) The date and time frame of the breach, if known; (9) The address and location of corporate headquarters, if outside of the District; (10) Any knowledge of foreign country involvement; and (11) A sample of the notice to be provided to District residents."	400 6th Street N.W. Washington, DC 20001	as defined by [15 U.S.C. § 1681a(p)], of the timing, distribution and content of the notices." "[The consumer reporting agency notice requirement] shall not apply to a person or entity who is required to notify consumer reporting agencies of a breach pursuant to [15 U.S.C. §§ 6801 et seq.]"

State & Statute	State Agency Notice Required; Contents	State Agency Notice Instructions; Address	Consumer Reporting Agency Notice Required; Contents
	"The notice required [to the Attorney General]… shall not be delayed on the grounds that the total number of District residents affected by the breach has not yet been ascertained."		
Guam 9 Guam Code §§ 48.20 – 48.50 (Jul. 11, 2009)	*(Not provided for.)*	*(N/A)*	*(Not provided for.)*
Puerto Rico P.R. Laws tit. 10, §§ 4051 – 4055 (Jun. 19, 2008)	"Within a non-extendable term of ten (10) days after the violation of the system's security has been detected, the parties responsible shall inform the Department [of Consumer Affairs]."	Mailing address: P.O. Box 41059, Minillas Station San Juan, PR 00940-1059 Physical address: Avenida José De Diego, Pda. 22 Centro Gubernamental Minillas, North Tower, 7th Floor Santurce, San Juan, PR 00909	*(Not provided for.)*
Virgin Islands V.I. Code tit. 14, § 2200, §§ 2209 – 2211 (Oct. 17, 2005)	*(Not provided for.)*	*(N/A)*	*(Not provided for.)*

Step 4 – What Are the Penalties?

[Back to Introduction]

State & Statute	Penalties; Liability
Alabama Ala. Code §§ 8-38-1 – 8-38-9, 8-38-11 – 8-38-12 (Jun. 1, 2018)	"A violation of the notification provisions of this [law] is an unlawful trade practice under the Alabama Deceptive Trade Practices Act, [Ala Code. §§ 8-19 et seq.]… The Attorney General shall have the exclusive authority to bring an action for civil penalties under this [law]." "[A] covered entity or third-party agent who is knowingly engaging in or has knowingly engaged in a violation of the notification provisions of this [law] will be subject to the penalty provisions set out in [Ala. Code § 8-19-11]. For the purposes of this [law, knowingly shall mean willfully or with reckless disregard in failing to comply with the notice requirements of [Ala Code §§ 8-38-5 – 8-38-6]. Civil penalties assessed under [Ala. Code § 8-19-11], shall not exceed five hundred thousand dollars ($500,000) per breach." "Notwithstanding any remedy available under [Ala. Code § 8-19-11 as described immediately above], a covered entity that violates the notification provisions of this [law] shall be liable for a civil penalty of not more than five thousand dollars ($5,000) per day for each consecutive day that the covered entity fails to take reasonable action to comply with the notice provisions of this [law]." "The office of the Attorney General shall have the exclusive authority to bring an action for damages in a representative capacity on behalf of any named individual or individuals. In such an action brought by the office of the Attorney General, recovery shall be limited to actual damages suffered by the person or persons, plus reasonable attorney's fees and costs." "To the extent that notification is required under this [law] as the result of a breach experienced by a third-party agent, a failure to inform the covered entity of the breach shall subject the third-party agent to the fines and penalties set forth in this [law]."
Alaska Alaska Stat. §§ 45.48.010 – 45.48.090 (Jul. 1, 2009)	"If an information collector… violates [Alaska Stat. §§ 45.48.010 – 45.48.090] with regard to the personal information of a state resident, the violation is an unfair or deceptive act or practice under [Alaska Stat. §§ 45.50.471 – 45.50.561]. However, (1) the information collector is not subject to the civil penalties imposed under [Alaska Stat. § 45.50.551] but is liable to the state for a civil penalty of up to $500 for each state resident who was not notified [as required]… except that the total civil penalty may not exceed $50,000; and (2) damages that may be awarded against the information collector under (A) [Alaska Stat. § 45.50.531] are limited to actual economic damages that do not exceed $500; and (B) [Alaska Stat. § 45.50.537] are limited to actual economic damages."
Arizona	"A knowing and wil[l]ful violation of [Ariz. Rev. Stat. § 18-552] is an unlawful practice pursuant to [Ariz. Rev. Stat. § 44-1522], and only the attorney general may enforce such a violation by investigating and taking appropriate action pursuant to [Ariz. Rev. Stat. §§ 44-1521 et seq.] The attorney general may impose a civil penalty for a violation of this [law] not to exceed the lesser of ten thousand dollars per affected individual or the total

State & Statute	Penalties; Liability
Ariz. Rev. Stat. § 18-551, § 18-552 (Aug. 3, 2018; as amended Mar 29, 2022)	amount of economic loss sustained by affected individuals, but the maximum civil penalty from a breach or series of related breaches may not exceed five hundred thousand dollars. This… does not prevent the attorney general from recovering restitution for affected individuals."
Arkansas Ark. Code §§ 4-110-101 – 4-110-108 (Jul. 23, 2019)	"[A] violation of [Ark. Code §§ 4-110-101 et seq.] is punishable by action of the Attorney General under the provisions of [Ark. Code §§ 4-88-101 et seq.]"
California Cal. Civ. Code § 1798.80, § 1798.82, § 1798.84, § 1798.150 (Jan. 1, 2021; § 1798.150 eff. Jan. 1, 2023)	"[A] customer injured by a violation of this [law] may institute a civil action to recover damages." "[A] business that violates, proposes to violate, or has violated this [law] may be enjoined." "The [immediately above] rights and remedies… are cumulative to each other and to any other rights and remedies available under law." "[A] consumer whose nonencrypted and nonredacted personal information, as defined in [Cal. Civ. Code § 1798.81.5(d)(1)(A), which is a subset of personal information as defined in § 1798.82(h)], or whose email address in combination with a password or security question and answer that would permit access to the account is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following: (A) To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater. (B) Injunctive or declaratory relief. (C) Any other relief the court deems proper." "In assessing the amount of statutory damages [in such a civil action], the court shall consider any one or more of the relevant circumstances presented by any of the parties to the case, including, but not limited to, the nature and seriousness of the misconduct, the number of violations, the

State & Statute	Penalties; Liability
	persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth." "[Such] [a]ctions… may be brought by a consumer if, prior to initiating any action against a business for statutory damages on an individual or class-wide basis, a consumer provides a business 30 days' written notice identifying the specific provisions of [Cal. Civ. Code § 1798.150(a)] the consumer alleges have been or are being violated. In the event a cure is possible, if within the 30 days the business actually cures the noticed violation and provides the consumer an express written statement that the violations have been cured and that no further violations shall occur, no action for individual statutory damages or class-wide statutory damages may be initiated against the business. The implementation and maintenance of reasonable security procedures and practices pursuant to [Cal. Civ. Code § 1798.81.5] following a breach does not constitute a cure with respect to that breach. [However,] [n]o notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages suffered as a result of the alleged violations of [Cal. Civ. Code § 1798.150(a)]… If a business continues… in breach of the express written statement provided to the consumer… the consumer may initiate an action against the business to enforce the written statement and may pursue statutory damages for each breach of the express written statement, as well as any other violation… that postdates the written statement." "The cause of action established [above]… shall apply only to violations [as provided for in Cal. Civ. Code § 1798.150(a)] and shall not be based on violations of any other section of [Cal. Civ. Code §§ 1798.100 et seq.] Nothing… shall be interpreted to serve as the basis for a private right of action under any other law."
Colorado Colo. Rev. Stat. § 6-1-716 (Sep. 1, 2018)	"The attorney general may bring an action in law or equity to address violations of this [law]… and for other relief that may be appropriate to ensure compliance with this [law] or to recover direct economic damages resulting from a violation, or both. The provisions of this [law] are not exclusive."
Connecticut Conn. Gen. Stat. § 36a-701b as amended by P.A. 21-59 (Oct. 1, 2021)	"Failure to comply with the requirements of this [law] shall constitute an unfair trade practice for purposes of [Conn. Gen. Stat. § 42-110b] and shall be enforced by the Attorney General."

Step 4 - What Are the Penalties?
[Back to Introduction]

State & Statute	Penalties; Liability
Delaware Del. Code tit. 6 §§ 12B-101 – 12B-104 (Apr. 14, 2018)	"Pursuant to the enforcement duties and powers of the Director of Consumer Protection of the Department of Justice under [Del. Code tit. 29, §§ 2501 et seq.] the Attorney General may bring an action in law or equity to address the violations of this [law] and for other relief that may be appropriate to ensure proper compliance with this [law] or to recover direct economic damages resulting from a violation, or both. The provisions of this [law] are not exclusive."
Florida Fla. Stat. § 501.171 (Oct. 1, 2019)	"A violation of [Fla. Stat. § 501.171] shall be treated as an unfair or deceptive trade practice in any action brought by the department [of legal affairs] under [Fla. Stat. § 501.207] against a covered entity or third-party agent." "In addition… a covered entity that violates [the department of legal affairs notice requirement] or [the individual notice requirement] shall be liable for a civil penalty not to exceed $500,000, as follows: 1. In the amount of $1,000 for each day up to the first 30 days following any violation of [such notice requirements] and, thereafter, $50,000 for each subsequent 30-day period or portion thereof for up to 180 days. 2. If the violation continues for more than 180 days, in an amount not to exceed $500,000. The civil penalties for failure to notify provided [immediately above]… apply per breach and not per individual affected by the breach." "This [law] does not establish a private cause of action."
Georgia Ga. Code § 10-1-911, § 10-1-912 (May 24, 2007)	*(Not provided for. Attorney General may levy fines for unfair/deceptive business practices, but have yet to do so in this context.)*
Hawai'i Haw. Rev. Code §§ 487N-1 – 487N-3 (Jul. 1, 2008)	"[A] business that violates any provision of this [law] shall be subject to penalties of not more than $2,500 for each violation. The attorney general or the executive director of the office of consumer protection may bring an action pursuant to this [law]." "In addition… [a] business that violates any provision of this [law] 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. The court in any action brought under this [law] may award reasonable attorneys' fees to the prevailing party."

State & Statute	Penalties; Liability
	"The penalties provided in this [law] shall be cumulative to the remedies or penalties available under all other laws of this State."
Idaho Idaho Code §§ 28-51-104 – 28-51-107 (Jul. 1, 2015)	"In [a] case in which… [a] commercial entity's or individual's primary regulator has reason to believe that an… individual or commercial entity subject to that primary regulator's jurisdiction under [Idaho Code § 28-51-104(6)] has violated [Idaho Code § 28-51-105] by failing to give notice in accordance with [Idaho Code § 28-51-105], the primary regulator may bring a civil action to enforce compliance with [Idaho Code § 28-51-105] and enjoin that… individual or commercial entity from further violations. [An]… individual or commercial entity that intentionally fails to give notice in accordance with [Idaho Code § 28-51-105] shall be subject to a fine of not more than twenty-five thousand dollars ($25,000) per breach of the security of the system." "'Primary regulator' of a commercial entity or individual licensed or chartered by the United States is that commercial entity's or individual's primary federal regulator, the primary regulator of a commercial entity or individual licensed by the department of finance is the department of finance, the primary regulator of a commercial entity or individual licensed by the department of insurance is the department of insurance and… for all other commercial entities or individuals, the primary regulator is the attorney general."
Illinois 815 Ill. Comp. Stat. §§ 530/1 – 530/10, §§ 530/15 – 530/20 (Jan. 1, 2020)	"A violation of this [law] constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act [found at 815 Ill. Comp. Stat. §§ 505/1 et seq.]"
Indiana Ind. Code §§ 24-4.9-1 – 24-4.9-5 (Jul. 1, 2017, as amended Mar. 18, 2022)	"A person that is required to make a disclosure or notification in accordance with [Ind. Code § 24-4.9-3] and that fails to comply with any provision of [Ind. Code §§ 24-4.9 et seq.] commits a deceptive act that is actionable only by the attorney general." "A failure to make a required disclosure or notification in connection with a related series of breaches of the security of data constitutes one (1) deceptive act. The attorney general may bring an action under [Ind. Code §§ 24-4.9-4 et seq.] to obtain any or all of the following: (1) An injunction to enjoin future violations of [Ind. Code §§ 24-4.9-3 et seq.] (2) A civil penalty of not more than one hundred fifty thousand dollars ($150,000) per deceptive act. (3) The attorney general's reasonable costs in: (A) the investigation of the deceptive act; and

State & Statute	Penalties; Liability
	(B) maintaining the action."
Iowa Iowa Code §§ 715C.1 – 715C.2 (Jul. 1, 2018)	"A violation of [Iowa Code §§ 715C.1 et seq.] is an unlawful practice pursuant to [Iowa Code § 714.16] and, in addition to the remedies provided to the attorney general pursuant to [Iowa Code § 714.16(7)], the attorney general may seek and obtain an order that a party held to violate [Iowa Code § 715C.2] pay damages to the attorney general on behalf of a person injured by the violation." "The rights and remedies available under [Iowa Code § 715C.2] are cumulative to each other and to any other rights and remedies available under the law."
Kansas Kan. Stat. §§ 50-7a01 – 50-7a02 (Jul. 1, 2006)	"For violations of [Kan. Stat. § 50-7a02], except as to insurance companies licensed to do business in this state, the attorney general is empowered to bring an action in law or equity to address violations of [Kan. Stat. § 50-7a02] and for other relief that may be appropriate. The provisions of [Kan. Stat. § 50-7a02] are not exclusive and do not relieve an individual or a commercial entity subject to [Kan. Stat. § 50-7a02] from compliance with all other applicable provisions of law." "For violations of [Kan. Stat. § 50-7a02] by an insurance company licensed to do business in this state, the insurance commissioner shall have the sole authority to enforce the provisions of [Kan. Stat. § 50-7a02]."
Kentucky Ky. Rev. Stat. § 365.732 (Jul. 15, 2014)	*(Not provided for. Fines may be issued for unfair/deceptive practices but have not yet in this context.)*
Louisiana La. Rev. Stat. §§ 51:3071 – 51:3077 (Aug. 1, 2018)	"A violation of a provision of [La. Rev. Stat. § 51:3074] shall constitute an unfair act or practice pursuant to [La. Rev. Stat. § 51:1405(A)]." "A civil action may be instituted to recover actual damages resulting from the failure to disclose in a timely manner to a person that there has been a breach of the security system resulting in the disclosure of a person's personal information." "Failure to provide timely notice [to the attorney general] may be punishable by a fine not to exceed $5,000 per violation… Each day notice is not received by the attorney general shall be deemed a separate violation."

State & Statute	Penalties; Liability
La. Admin. Code tit. 16, pt. III, § 701 (Mar. 20, 2007)	
Maine Me. Stat. tit. 10, §§ 1346 – 1350-A (Sep. 19, 2019)	"The appropriate state regulators within the Department of Professional and Financial Regulation shall enforce [Me. Stat. tit. 10, §§ 1346 et seq.] for any person that is licensed or regulated by those regulators. The Attorney General shall enforce [Me. Stat. tit. 10, §§ 1346 et seq.] for all other persons." "A person that violates [Me. Stat. tit. 10, §§ 1346 et seq.] commits a civil violation and is subject to one or more of the following: A. 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 [Me. Stat. tit. 10, §§ 1346 et seq.]…; B. Equitable relief; or C. Enjoinment from further violations of [Me. Stat. tit. 10, §§ 1346 et seq.]" "The rights and remedies available under [Me. Stat. tit. 10, § 1349] are cumulative and do not affect or prevent rights and remedies available under federal or state law."
Maryland Md. Com. Law §§ 14-3501 – 14-3508 (Oct. 1, 2022)	"A violation of [Md. Com. Law §§ 14-3501 et seq.]: (1) Is an unfair or deceptive trade practice within the meaning of [Md. Com. Law §§ 13-101 et seq.]; and (2) Is subject to the enforcement and penalty provisions contained in [Md. Com. Law §§ 13-101 et seq.]"
Massachusetts Mass. Gen. Laws §§ 93H-1 – 93H-6 (Apr. 10, 2019)	"The attorney general may bring an action pursuant to [Mass. Gen. Laws § 93A-4] against a person or otherwise to remedy violations of [Mass. Gen. Laws §§ 93H-1 et seq.] and for other relief that may be appropriate."
Michigan	"A person that provides notice of a security breach in the manner described in [Mich. Comp. Laws § 445.72] when a security breach has not occurred, with the intent to defraud, is guilty of a misdemeanor punishable as follows:

State & Statute	Penalties; Liability
Mich. Comp. Laws §§ 445.61 – 445.64, § 445.72, § 445.72b (Jan. 1, 2020)	(a) Except as otherwise provided under [the immediately below] subdivisions (b) and (c), by imprisonment for not more than 93 days or a fine of not more than $250.00 for each violation, or both. (b) For a second violation, by imprisonment for not more than 93 days or a fine of not more than $500.00 for each violation, or both. (c) For a third or subsequent violation, by imprisonment for not more than 93 days or a fine of not more than $750.00 for each violation, or both." "[A] person that knowingly fails to provide any notice of a security breach required under [Mich. Comp. Laws § 445.72] may be ordered to pay a civil fine of not more than $250.00 for each failure to provide notice. The attorney general or a prosecuting attorney may bring an action to recover a civil fine under [Mich. Comp. Laws § 445.72]… [but] [t]he aggregate liability of a person for [such] civil fines… for multiple [such] violations… that arise from the same security breach shall not exceed $750,000.00. "[The above remedies] do not affect the availability of any civil remedy for a violation of state or federal law." "A person who knowingly or intentionally violates [Mich. Comp. Laws § 445.72b] is guilty of a misdemeanor punishable as follows: (a) Except as otherwise provided in [the immediately below] subdivisions (b) and (c), by imprisonment for not more than 93 days or a fine of not more than $1,000.00 for each violation, or both. (b) For a second violation, by imprisonment for not more than 93 days or a fine of not more than $2,000.00 for each violation, or both. (c) For a third or subsequent violation, by imprisonment for not more than 93 days or a fine of not more than $3,000.00 for each violation, or both." "[The immediately above remedy] does not affect the availability of any civil remedy for a violation of [Mich. Comp. Laws § 445.72] or any other state or federal law."
Minnesota Minn. Stat. § 325E.61 (Jul. 1, 2006)	"The attorney general shall enforce [Minn. Stat. § 325E.61]… under [Minn. Stat. § 8.31]."
Mississippi Miss. Code § 75-24-29 (Jul. 1, 2021)	"Failure to comply with the requirements of [Miss. Code § 75-24-29] shall constitute an unfair trade practice and shall be enforced by the Attorney General; however, nothing in [Miss. Code § 75-24-29] may be construed to create a private right of action."

State & Statute	Penalties; Liability
Missouri Mo. Rev. Stat. § 407.1500 (Aug. 28, 2009)	"The attorney general shall have exclusive authority to bring an action to obtain actual damages for a willful and knowing violation of [Mo. Rev. Stat. § 407.1500] and may seek a civil penalty not to exceed one hundred fifty thousand dollars per breach of the security of the system or series of breaches of a similar nature that are discovered in a single investigation."
Montana Mont. Code § 30-14-1702, §§ 30-14-1704 – 30-14-1705 (Oct. 1, 2015)	"Whenever the department [of justice] has reason to believe that a person has violated [Mont. Code §§ 30-14-1701 et seq.] and that proceeding would be in the public interest, the department may bring an action in the name of the state against the person to restrain by temporary or permanent injunction or temporary restraining order the use of the unlawful method, act, or practice upon giving appropriate notice to that person pursuant to [Mont. Code § 30-14-111(2)]." "A violation of [Mont. Code §§ 30-14-1701 et seq.] is a violation of [Mont. Code § 30-14-103], and the penalties for a violation of [Mont. Code §§ 30-14-1701 et seq.] are as provided in [Mont. Code § 30-14-142]." "The provisions of [Mont. Code § 30-14-111(3)–(4), §§ 30-14-112 – 30-14-115] apply to [Mont. Code §§ 30-14-1701 et seq.]"
Nebraska Neb. Rev. Stat. §§ 87-801 – 87-807 (Jul. 18, 2018)	"For purposes of [this law], the Attorney General may issue subpoenas and seek and recover direct economic damages for each affected Nebraska resident injured by a violation of [Neb. Rev. Stat. § 87-803]."
Nevada Nev. Rev. Stat. §§ 603A.010 – 603A.100, §§ 603A.215 – 603A.290 (Oct. 1, 2021)	"If the Attorney General or a district attorney of any county has reason to believe that any person is violating, proposes to violate or has violated the provisions of [Nev. Rev. Stat. §§ 603A.010 – 603A.290], the Attorney General or district attorney may bring an action against that person to obtain a temporary or permanent injunction against the violation." "A data collector shall not be liable for damages for a breach of the security of the system data if: (a) The data collector is in compliance with [Nev. Rev. Stat. § 603A.215]; and (b) The breach is not caused by the gross negligence or intentional misconduct of the data collector, its officers, employees or agents.

State & Statute	Penalties; Liability
New Hampshire N.H. Rev. Stat. §§ 359-C:19 – 359-C:21 (Jan. 1, 2007)	"[A] person injured by any violation under [N.H. Rev. Stat. §§ 359-C:19 et seq.] 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 for the plaintiff, recovery shall be in the amount of actual damages. If the court finds that the act or practice was a willful or knowing violation of [N.H. Rev. Stat. §§ 359-C:1 et seq.], it shall award as much as 3 times, but not less than 2 times, such amount. In addition, a prevailing plaintiff shall be awarded the costs of the suit and reasonable attorney's fees, as determined by the court. Any attempted waiver of the right to [such] damages… shall be void and unenforceable. Injunctive relief shall be available to private individuals under [N.H. Rev. Stat. §§ 359-C:1 et seq.] without bond, subject to the discretion of the court." "The New Hampshire attorney general's office shall enforce the provisions of [N.H. Rev. Stat. §§ 359-C:19 et seq.] pursuant to [N.H. Rev. Stat. § 358-A:4]." "The burden shall be on the person responsible for the determination under [N.H. Rev. Stat. § 359-C:20(I)] to demonstrate compliance with [N.H. Rev. Stat. §§ 359-C:19 et seq.]"
New Jersey N.J. Stat. § 56:8-161, § 56:8-163, §§ 56:8-165 – 56:8-166 (Sep. 1, 2019)	"It shall be an unlawful practice and a violation of [N.J. Stat. §§ 56:8-1 et seq.] to willfully, knowingly or recklessly violate [N.J. Stat. §§ 56:8-161 – 56:8-164]."
New Mexico N.M. Stat. §§ 57-12C-1 – 57-12C-2, §§ 57-12C-6 – 57-12C-11 (Jun. 16, 2017)	"When the attorney general has a reasonable belief that a violation of [this law] has occurred, the attorney general may bring an action on the behalf of individuals and in the name of the state alleging a violation of [this law]." "In any [such] action filed by the attorney general… the court may: (1) issue an injunction; and (2) award damages for actual costs or losses, including consequential financial losses." "If the court determines that a person violated [this law] knowingly or recklessly, the court may impose a civil penalty of the greater of twenty five thousand dollars ($25,000) or, in the case of failed notification, ten dollars ($10.00) per instance of failed notification up to a maximum of one hundred fifty thousand dollars ($150,000)."

State & Statute	Penalties; Liability
New York N.Y. Gen. Bus. Law § 899-AA (Oct. 23, 2019)	"[W]henever the attorney general shall believe from evidence satisfactory to him or her that there is a violation of [N.Y. Gen. Bus. Law § 899-AA] he or she may bring an action in the name and on behalf of the people of the state of New York, in a court of justice having jurisdiction to issue an injunction, to enjoin and restrain the continuation of such violation. In such action, preliminary relief may be granted under [N.Y. C.P.L.R. Law §§ 6301 et seq.] In such action the court may award damages for actual costs or losses incurred by a person entitled to [individual] notice… if [such] notification was not provided to such person… including consequential financial losses. Whenever the court shall determine in such action that a person or business violated [N.Y. Gen. Bus. Law § 899-AA] knowingly or recklessly, the court may impose a civil penalty of the greater of five thousand dollars or up to twenty dollars per instance of failed notification, provided that the latter amount shall not exceed two hundred fifty thousand dollars." "[T]he remedies provided [herein] shall be in addition to any other lawful remedy available." "[But] no [such] action may be brought… unless such action is commenced within three years after either the date on which the attorney general became aware of the violation, or the date of notice sent [to the attorney general by the person or business]… whichever occurs first. In no event shall an action be brought after six years from the date of discovery of the breach of private information by the company unless the company took steps to hide the breach."
North Carolina N.C. Gen. Stat. § 75-60, § 75-61, § 75-65 (Jan. 1, 2016)	"A violation of [N.C. Gen. Stat. § 75-65] is a violation of [N.C. Gen. Stat. § 75-1.1]. No private right of action may be brought by an individual for a violation of [N.C. Gen. Stat. § 75-65] unless such individual is injured as a result of the violation." "Causes of action arising under [N.C. Gen. Stat. §§ 75-60 et seq.] may not be assigned."
North Dakota N.D. Cent. Code §§ 51-30-01 – 51-30-07 (Aug. 1, 2015)	"The attorney general may enforce [N.D. Cent. Code §§ 51-30-01 et seq.] The attorney general, in enforcing [N.D. Cent. Code §§ 51-30-01 et seq.], has all the powers provided in [N.D. Cent. Code §§ 51-15-01 et seq.] and may seek all the remedies in [N.D. Cent. Code §§ 51-15-01 et seq.] A violation of [N.D. Cent. Code §§ 51-30-01 et seq.] is deemed a violation of [N.D. Cent. Code §§ 51-15-01 et seq.] The remedies, duties, prohibitions, and penalties of [N.D. Cent. Code §§ 51-30-01 et seq.] are not exclusive and are in addition to all other causes of action, remedies, and penalties under [N.D. Cent. Code §§ 51-15-01 et seq.], or otherwise provided by law."
Ohio	"The attorney general may conduct pursuant to [Ohio Rev. Code §§ 1349.191 – 1349.192] an investigation and bring a civil action upon an alleged failure by a person to comply with the requirements of [Ohio Rev. Code § 1349.19]."

State & Statute	Penalties; Liability
Ohio Rev. Code §§ 1349.19 – 1349.192 (Mar. 30, 2007)	"The attorney general shall have the exclusive authority to bring a civil action in a court of common pleas for appropriate relief under [Ohio Rev. Code § 1349.92], including a temporary restraining order, preliminary or permanent injunction, and civil penalties, if it appears that… a person has failed or is failing to comply with [Ohio Rev. Code § 1349.19]. Upon its finding that a… person has failed to comply with [Ohio Rev. Code § 1349.19], the court shall impose a civil penalty upon the… person as follows: (a) For each day that the… person has intentionally or recklessly failed to comply with the applicable section, subject to [the immediately below] divisions [(b) and (c)]…, a civil penalty of up to one thousand dollars for each day the… person fails to comply with the section; (b) If the… person has intentionally or recklessly failed to comply with the applicable section for more than sixty days, subject to [the immediately below] division [(c)]… a civil penalty [of up to one thousand dollars for each day]… for each day of the first sixty days that the… person fails to comply with the section and, for each day commencing with the sixty-first day that the… person has failed to comply with the section, a civil penalty of up to five thousand dollars for each such day the… person fails to comply with the section; (c) If the… person has intentionally or recklessly failed to comply with the applicable section for more than ninety days, a civil penalty [of up to one thousand dollars for each day]… for each day of the first sixty days that the… person fails to comply with the section, a civil penalty of up to five thousand dollars for each day commencing with the sixty-first day and continuing through the ninetieth day that the… person fails to comply with the section, and, for each day commencing with the ninety-first day that the… person has failed to comply with the section, a civil penalty of up to ten thousand dollars for each such day the… person fails to comply with the section." "In determining the appropriate civil penalty to assess under [the above schedule]… the court shall consider all relevant factors, including the following: (a) If the defendant in the civil action is… a person that is a business entity, whether or not the high managerial officer, agent, or employee of the agency or business entity having supervisory responsibility for compliance with [Ohio Rev. Code § 1347.12 or § 1349.19], whichever is applicable, acted in bad faith in failing to comply with the section. (b) If the defendant in the civil action is a person other than a business entity, whether or not the person acted in bad faith in failing to comply with [Ohio Rev. Code § 1349.19]. "The [above] rights and remedies… are in addition to any other rights or remedies that are provided by law."
Oklahoma Okla. Stat. tit. 24, §§ 161 – 166 (Nov. 1, 2008)	"A violation of this [law] that results in injury or loss to residents of this state may be enforced by the Attorney General or a district attorney in the same manner as an unlawful practice under the Oklahoma Consumer Protection Act [found at Okla. Stat. tit. 15, §§ 751 et seq.]" "[T]he Attorney General or a district attorney shall have exclusive authority to bring action and may obtain either actual damages for a violation of this [law] or a civil penalty not to exceed One Hundred Fifty Thousand Dollars ($150,000.00) per breach of the security of the system or series of breaches of a similar nature that are discovered in a single investigation… [but] [a] violation of this [law] by a state-chartered or state-licensed financial institution shall be enforceable exclusively by the primary state regulator of the financial institution."

State & Statute	Penalties; Liability
Oregon Or. Rev. Stat. §§ 646A.600 – 646A.604, 646A.624 – 646A.628 (Jan. 1, 2020)	"A person's violation of a provision of [Or. Rev. Stat. §§ 646A.600 – 646A.628] is an unlawful practice under [Or. Rev. Stat. § 646.607]… [such] rights and remedies… are cumulative and are in addition to any other rights or remedies that are available under law." "If the director [of the Department of Consumer and Business Services] has reason to believe that any person has engaged or is engaging in any violation of [Or. Rev. Stat. §§ 646A.600 – 646A.628], the director may issue an order, subject to [Or. Rev. Stat. §§ 183.310 et seq.], directed to the person to cease and desist from the violation, or require the person to pay compensation to consumers injured by the violation. The director may order compensation to consumers only upon a finding that enforcement of the rights of the consumers by private civil action would be so burdensome or expensive as to be impractical." "In addition to all other penalties and enforcement provisions provided by law, any person who violates or who procures, aids or abets in the violation of [Or. Rev. Stat. §§ 646A.600 – 646A.628] shall be subject to a penalty of not more than $1,000 for every violation… [e]very [such] violation is a separate offense and, in the case of a continuing violation, each day's continuance is a separate violation, but the maximum penalty for any occurrence shall not exceed $500,000." "Civil penalties under [Or. Rev. Stat. § 646A.624] shall be imposed as provided in [Or. Rev. Stat. § 183.745]."
Pennsylvania 73 Pa. Cons. Stat. §§ 2301 – 2330 (May 2, 2023)	"A violation of this [law] shall be deemed to be an unfair or deceptive act or practice in violation of [73 Pa. Cons. Stat. §§ 201-1 et seq.]… known as the Unfair Trade Practices and Consumer Protection Law. The Office of Attorney General shall have exclusive authority to bring an action under the Unfair Trade Practices and Consumer Protection Law for a violation of this [law]."
Rhode Island R.I. Gen. Laws § 11-49.3-1, §§ 11-49.3-3 – 11-49.3-6 (Jul. 2, 2016)	"Each reckless violation of [R.I. Gen. Laws §§ 11-49.3-1 et seq.] is a civil violation for which a penalty of not more than one hundred dollars ($100) per record may be adjudged against a defendant." "Each knowing and willful violation of [R.I. Gen. Laws §§ 11-49.3-1 et seq.] is a civil violation for which a penalty of not more than two hundred dollars ($200) per record may be adjudged against a defendant." "Whenever the attorney general has reason to believe that a violation of [R.I. Gen. Laws §§ 11-49.3-1 et seq.] has occurred and that proceedings would be in the public interest, the attorney general may bring an action in the name of the state against the business or person in violation."

State & Statute	Penalties; Liability
South Carolina S.C. Code § 39-1-90 (Apr. 23, 2013)	"A person who knowingly and willfully violates [S.C. Code § 39-1-90] is subject to an administrative fine in the amount of one thousand dollars for each resident whose information was accessible by reason of the breach, the amount to be decided by the Department of Consumer Affairs." "A resident of this State who is injured by a violation of [S.C. Code § 39-1-90], in addition to and cumulative of all other rights and remedies available at law, may: (1) institute a civil action to recover damages in case of a wil[l]ful and knowing violation; (2) institute a civil action that must be limited to actual damages resulting from a violation in case of a negligent violation of [S.C. Code § 39-1-90]; (3) seek an injunction to enforce compliance; and (4) recover attorney's fees and court costs, if successful."
South Dakota S.D. Cod. Laws §§ 22-40-19 – 22-40-26 (Jul. 1, 2018)	"The attorney general may prosecute each failure to disclose under the provisions of [S.D. Cod. Laws §§ 22-40-19 – 22-40-26], inclusive, as a deceptive act or practice under [S.D. Cod. Laws § 37-24-6]. In addition to any remedy provided under [S.D. Cod. Laws §§ 37-24-1 et seq.], the attorney general may bring an action to recover on behalf of the state a civil penalty of not more than ten thousand dollars per day per violation. The attorney general may recover attorney's fees and any costs associated with any action brought under [S.D. Cod. Laws § 22-40-25]."
Tennessee Tenn. Code § 47-18-2107 (Apr. 4, 2017)	"[A] customer of an information holder who is a person or business entity… and who is injured by a violation of [Tenn. Code § 47-18-2107], may institute a civil action to recover damages and to enjoin the information holder from further action in violation of [Tenn. Code § 47-18-2107]. The rights and remedies available under [Tenn. Code § 47-18-2107] are cumulative to each other and to any other rights and remedies available under law."
Texas Tex. Bus. & Com. Code § 521.002, § 521.053, § 521.151 (As amended by SB 768, effective Sep. 1, 2023)	"A person who violates [Tex. Bus. & Com. Code §§ 521.001 et seq.] is liable to this state for a civil penalty of at least $2,000 but not more than $50,000 for each violation. The attorney general may bring an action to recover [such] civil penalty." "In addition… a person who fails to take reasonable action to comply with [the individual notice requirement] is liable to this state for a civil penalty of not more than $100 for each individual to whom [individual] notification is due… for each consecutive day that the person fails to take reasonable action to comply with that [the individual notice requirement]. Civil penalties under [Tex. Bus. & Com. Code § 521.151] may not exceed $250,000 for all individuals to whom notification is due after a single breach. The attorney general may bring an action to recover [such] civil penalties."

State & Statute	Penalties; Liability
	"If it appears to the attorney general that a person is engaging in, has engaged in, or is about to engage in conduct that violates [Tex. Bus. & Com. Code §§ 521.001 et seq.], the attorney general may bring an action in the name of the state against the person to restrain the violation by a temporary restraining order or by a permanent or temporary injunction. "In an action under [Tex. Bus. & Com. Code § 521.151], the court may grant any other equitable relief that the court considers appropriate to: (1) prevent any additional harm to a victim of identity theft or a further violation of [Tex. Bus. & Com. Code §§ 521.001 et seq.]; or (2) satisfy any judgment entered against the defendant, including issuing an order to appoint a receiver, sequester assets, correct a public or private record, or prevent the dissipation of a victim's assets. "The attorney general is entitled to recover reasonable expenses, including reasonable attorney's fees, court costs, and investigatory costs, incurred in obtaining injunctive relief or civil penalties, or both, under [Tex. Bus. & Com. Code § 521.151]." "The fees associated with an action under [Tex. Bus. & Com. Code § 521.151] are the same as in a civil case, but the fees may be assessed only against the defendant."
Utah Utah Code §§ 13-44-101 – 13-44-103, § 13-44-202, § 13-44-301 (May 3, 2023)	"The attorney general may enforce [Utah Code §§ 13-44-01 et seq.]'s provisions." "Nothing in [Utah Code §§ 13-44-01 et seq.] creates a private right of action… [or] affects any private right of action existing under other law, including contract or tort." "A person who violates [Utah Code §§ 13-44-01 et seq.]'s provisions is subject to a civil penalty of: (a) no greater than $2,500 for a violation or series of violations concerning a specific consumer; and (b) no greater than $100,000 in the aggregate for related violations concerning more than one consumer, unless: (i) the violations concern: (A) 10,000 or more consumers who are residents of the state; and (B) 10,000 or more consumers who are residents of other states; or (ii) the person agrees to settle for a greater amount." "In addition… the attorney general may seek, in an action brought under [Utah Code §§ 13-44-01 et seq.]: (i) injunctive relief to prevent future violations of [Utah Code §§ 13-44-01 et seq.]; and (ii) attorney fees and costs."

State & Statute	Penalties; Liability
	"A civil action under [Utah Code §§ 13-44-01 et seq.] shall be commenced no later than five years after the day on which the alleged breach of system security last occurred." "'Consumer' means a natural person."
Vermont Vt. Stat. tit. 9, § 2430, § 2435 (Jul. 1, 2020)	"With respect to all data collectors and other entities subject to [Vt. Stat. tit. 9, § 2435], other than a person or entity licensed or registered with the Department of Financial Regulation under [Vt. Stat. tit. 9, §§ 1 et seq. or tit. 8, §§ 1 et seq.], the Attorney General and State's Attorney shall have sole and full authority to investigate potential violations of [Vt. Stat. tit. 9, § 2435] and to enforce, prosecute, obtain, and impose remedies for a violation of [Vt. Stat. tit. 9, § 2435] or any rules or regulations made pursuant to [Vt. Stat. tit. 9, §§ 2430 et seq.] as the Attorney General and State's Attorney have under [Vt. Stat. tit. 9, §§ 2451 et seq.] The Attorney General may refer the matter to the State's Attorney in an appropriate case." "With respect to a data collector that is a person or entity licensed or registered with the Department of Financial Regulation under [Vt. Stat. tit. 9, §§ 1 et seq. or tit. 8, §§ 1 et seq.], the Department of Financial Regulation shall have the full authority to investigate potential violations of [Vt. Stat. tit. 9, § 2435] and to prosecute, obtain, and impose remedies for a violation of [Vt. Stat. tit. 9, § 2435] or any rules or regulations adopted pursuant to [Vt. Stat. tit. 9, § 2435], as the Department has under [Vt. Stat. tit. 9, §§ 1 et seq. or tit. 8, §§ 1 et seq.] or any other applicable law or regulation."
Virginia Va. Code § 18.2-186.6 (Jul. 1, 2020)	"[P]ursuant to the enforcement duties and powers of the Office of the Attorney General, the Attorney General may bring an action to address violations of [Va. Code § 18.2-186.6]. The Office of the Attorney General may impose a civil penalty not to exceed $150,000 per breach of the security of the system or a series of breaches of a similar nature that are discovered in a single investigation. Nothing in [Va. Code § 18.2-186.6] shall limit an individual from recovering direct economic damages from a violation of [Va. Code § 18.2-186.6]… [but] [a] violation of [Va. Code § 18.2-186.6] by a state-chartered or licensed financial institution shall be enforceable exclusively by the financial institution's primary state regulator… [and] [n]othing in [Va. Code § 18.2-186.6] shall apply to an individual or entity regulated by the State Corporation Commission's Bureau of Insurance." "The Attorney General shall have exclusive authority to enforce the provisions of [Va. Code § 59.1-575(A)(2)]." "Prior to initiating any action under [Va. Code §§ 59.1-571 et seq.], the Attorney General shall provide a controller or processor 30 days' written notice identifying the specific provisions of [Va. Code §§ 59.1-571 et seq.] the Attorney General alleges have been or are being violated. If within the 30-day period, the controller or processor cures the noticed violation and provides the Attorney General an express written statement that the alleged violations have been cured and that no further violations shall occur, no action shall be initiated against the controller or processor."

State & Statute	Penalties; Liability
	"If a controller or processor continues to violate [Va. Code § 59.1-575(A)(2)] following the cure period… or breaches [the related] express written statement provided to the Attorney General… the Attorney General may initiate an action in the name of the Commonwealth and may seek an injunction to restrain any violations of [Va. Code § 59.1-575(A)(2)] and civil penalties of up to $7,500 for each [such] violation." "The Attorney General may recover reasonable expenses incurred in investigating and preparing the case, including attorney fees, in any action initiated under [Va. Code §§ 59.1-571 et seq.]" "Nothing in [Va. Code §§ 59.1-571 et seq.] shall be construed as providing the basis for, or be subject to, a private right of action for violations of [Va. Code § 59.1-575(A)(2)] or under any other law."
Washington Wash. Rev. Code §§ 19.255.005 – 19.255.040 (Mar. 1, 2020)	"[A] consumer injured by a violation of [Wash. Rev. Code §§ 19.255.005 et seq.] may institute a civil action to recover damages." "[A] person or business that violates, proposes to violate, or has violated [Wash. Rev. Code §§ 19.255.005 et seq.] may be enjoined." "The attorney general may bring an action in the name of the state, or as *parens patriae* on behalf of persons residing in the state, to enforce [Wash. Rev. Code §§ 19.255.005 et seq.] For actions brought by the attorney general to enforce [Wash. Rev. Code §§ 19.255.005 et seq.], the legislature finds that the practices covered by [Wash. Rev. Code §§ 19.255.005 et seq.] are matters vitally affecting the public interest for the purpose of applying the consumer protection act, [Wash. Rev. Code §§ 19.86.010 et seq.] For actions brought by the attorney general to enforce [Wash. Rev. Code §§ 19.255.005 et seq.], a violation of [Wash. Rev. Code §§ 19.255.005 et seq.] is not reasonable in relation to the development and preservation of business and is an unfair or deceptive act in trade or commerce and an unfair method of competition for purposes of applying the consumer protection act, [Wash. Rev. Code §§ 19.86.010 et seq.] An action to enforce [Wash. Rev. Code §§ 19.255.005 et seq.] may not be brought under [Wash. Rev. Code § 19.86.090]." "The rights and remedies available under [Wash. Rev. Code §§ 19.255.005 et seq.] are cumulative to each other and to any other rights and remedies available under law." "Processors, businesses, and vendors are not liable under [Wash. Rev. Code § 19.255.020] if (a) the account information was encrypted at the time of the breach, or (b) the processor, business, or vendor was certified compliant with the payment card industry data security standards adopted by the payment card industry security standards council, and in force at the time of the breach." "If a processor or business fails to take reasonable care to guard against unauthorized access to account information that is in the possession or under the control of the business or processor, and the failure is found to be the proximate cause of a breach, the processor or business is liable to a financial institution for reimbursement of reasonable actual costs related to the reissuance of credit cards and debit cards that are incurred by the financial

State & Statute	Penalties; Liability
	institution to mitigate potential current or future damages to its credit card and debit card holders that reside in the state of Washington as a consequence of the breach, even if the financial institution has not suffered a physical injury in connection with the breach. In any [such] legal action… the prevailing party is entitled to recover its reasonable attorneys' fees and costs incurred in connection with the legal action." "A vendor, instead of a processor or business, is liable to a financial institution for the damages described [immediately above]… to the extent that the damages were proximately caused by the vendor's negligence and if the claim is not limited or foreclosed by another provision of law or by a contract to which the financial institution is a party." "The remedies under [Wash. Rev. Code § 19.255.020] are cumulative and do not restrict any other right or remedy otherwise available under law, however a trier of fact may reduce damages awarded to a financial institution by any amount the financial institution recovers from a credit card company in connection with the breach, for costs associated with access card reissuance." "[For purposes of Wash. Rev. Code § 19.255.020], '[b]usiness' means an individual, partnership, corporation, association, organization… or any other legal or commercial entity that processes more than six million credit card and debit card transactions annually, and who provides, offers, or sells goods or services to persons who are residents of Washington… '[e]ncrypted' means enciphered or encoded using standards reasonable for the breached business or processor taking into account the business or processor's size and the number of transactions processed annually… '[p]rocessor' means an individual, partnership, corporation, association, organization… or any other legal or commercial entity, other than a business as defined [immediately above], that directly processes or transmits account information for or on behalf of another person as part of a payment processing service… [and] '[v]endor' means an individual, partnership, corporation, association, organization… or any other legal or commercial entity that manufactures and sells software or equipment that is designed to process, transmit, or store account information or that maintains account information that it does not own." "'Account information' means: (i) The full, unencrypted magnetic stripe of a credit card or debit card; (ii) the full, unencrypted account information contained on an identification device as defined under [Wash. Rev. Code § 19.300.010]; or (iii) the unencrypted primary account number on a credit card or debit card or identification device, plus any of the following if not encrypted: Cardholder name, expiration date, or service code."
West Virginia W. Va. Code §§ 46A-2A-101 – 46A-2A-105 (Jun. 7, 2008)	"[F]ailure to comply with the notice provisions of [W. Va. Code §§ 46A-2A-101 et seq.] constitutes an unfair or deceptive act of practice in violation of [W. Va. Code § 46A-6-104], which may be enforced by the Attorney General pursuant to the enforcement provisions of [W. Va. Code §§ 46A-1-101 et seq.]… [but] [a] violation of [W. Va. Code §§ 46A-2A-101 et seq.] by a licensed financial institution shall be enforceable exclusively by the financial institution's primary functional regulator." "[T]he Attorney General shall have exclusive authority to bring action. No civil penalty may be assessed in an action unless the court finds that the defendant has engaged in a course of repeated and willful violations of [W. Va. Code §§ 46A-2A-101 et seq.] No civil penalty shall exceed $150,000 per

State & Statute	Penalties; Liability
	breach of security of the system or series of breaches of a similar nature that are discovered in a single investigation… [However,] [a] violation of [W. Va. Code §§ 46A-2A-101 et seq.] by a licensed financial institution shall be enforceable exclusively by the financial institution's primary functional regulator."
Wisconsin Wis. Stat. §§ 134.98 – 134.99 (Mar. 28, 2008)	"Failure to comply with [Wis. Stat. § 134.98] is not negligence or a breach of any duty, but may be evidence of negligence or a breach of a legal duty." "Whoever is concerned in the commission of a violation of [Wis. Stat. § 134.98] for which a forfeiture is imposed is a principal and may be charged with and convicted of the violation although he or she did not directly commit it and although the person who directly committed it has not been convicted of the violation… A person is concerned in the commission of the violation if the person: (a) Directly commits the violation; (b) Aids and abets the commission of it; or (c) Is a party to a conspiracy with another to commit it or advises, hires or counsels or otherwise procures another to commit it."
Wyoming Wyo. Stat. §§ 40-12-501 – 40-12-502 (Jul. 1, 2015) Wyo. Stat. § 6-3-901(b)(iii)–(xiv) (Jul. 1, 2015)	"The attorney general may bring an action in law or equity to address any violation of [Wyo. Stat. § 40-12-502] and for other relief that may be appropriate to ensure proper compliance with [Wyo. Stat. § 40-12-502], to recover damages, or both. The provisions of [Wyo. Stat. § 40-12-502] are not exclusive."
District of Columbia D.C. Code §§ 28-3851 – 28-3853 (Jun. 17, 2020)	"A violation of [D.C. Code §§ 28-3851 et seq.], or any rule issued pursuant to the authority of [D.C. Code §§ 28-3851 et seq.], is an unfair or deceptive trade practice pursuant to [D.C. Code § 28-3904(kk)]." "The [above] rights and remedies… are cumulative to each other and to any other rights and remedies available under law."
Guam	"A violation of [Guam Code §§ 48.10 et seq.] that results in injury or loss to residents of Guam may be enforced by the Office of the Attorney General."

Step 4 - What Are the Penalties?
[Back to Introduction]

State & Statute	Penalties; Liability
9 Guam Code §§ 48.20 – 48.50 (Jul. 11, 2009)	"[T]he Office of the Attorney General shall have exclusive authority to bring action and may obtain either actual damages for a violation of [Guam Code §§ 48.10 et seq.] or a civil penalty not to exceed One Hundred Fifty Thousand Dollars ($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."
Puerto Rico P.R. Laws tit. 10, §§ 4051 – 4055 (Jun. 19, 2008)	"The Secretary [of the Department of Consumer Affairs] may impose fines of five hundred dollars ($500) up to a maximum of five thousand dollars ($5,000) for each violation of the provisions of [P.R. Laws tit. 10, §§ 4051 et seq.] or its regulations… [such] fines… do not affect the rights of the consumers to initiate actions or claims for damages before a competent court."
Virgin Islands V.I. Code tit. 14, § 2200, §§ 2209 – 2211 (Oct. 17, 2005)	"[A] customer injured by a violation of [V.I. Code tit. 14, §§ 1 et seq.] may commence a civil action to recover damages." "[A] business that violates, proposes to violate, or has violated [V.I. Code tit. 14, §§ 1 et seq.] may be enjoined." "The [above] rights and remedies… are cumulative to each other and to any other rights and remedies available under law."

■