

Data Breach Notification in the **United States and Territories**



Privacy Rights
Clearinghouse



Given the daily barrage of data breaches impacting consumers, Americans are increasingly demanding stronger privacy protections. In 2002, California became the first state to recognize the need for individuals to be made aware when their data is exposed in security incidents. Sixteen years later, in 2018, South Dakota and Alabama finally became the 49th and 50th states, respectively, to enact data breach notification statutes to protect their residents.

However, not every American enjoys the same level of protections in their respective state. We took a close look at the current landscape of data breach notification statutes across the country, and identified key disparities in the level of protections that each statute affords.

Our analysis compares each state's data breach notification statutes along key provisions, including:

- definition of *breach*;
- definition of *personally identifiable information*;
- form of data covered;
- whether the statute covers paper records;
- whether the statute covers encrypted data when the encryption key has been accessed or acquired;
- what entities are covered by the statute;
- whether notification triggers after discovery or after reasonable investigation;
- whether there is a *risk of harm* trigger for notification;
- how consumers are notified;
- what must be included in the notice;
- whom entities must notify;
- whether the state publishes breach data publicly;
- whether individuals have a private right of action for violations;
- whether there are exceptions to the notification obligation if entity complies with other laws (HIPPA, GLB, etc);
- whether there is flexibility in notification if the entity maintains equivalent or stronger policy; and
- penalties for violations.

States and Territories

Alabama	4	Kentucky	44	Ohio	80	Appendix: Data Visualizations and Grades States Covering Paper Records118 States Requiring Notification When Both Encrypted Data and the Encryption Key are Exposed.....119 States with Personal Information Definition Including Medical Information120 States with Personal Information Definition Including Biometric Information 121 States with Personal Information Definition Including Passport Information122 States and Territories Allowing a Breach Entity to Avoid Notifying if it Determines There is <i>No Reasonable Likelihood of Harm</i> to Residents.....123 States and Territories Requiring Notification to the Attorney General124 States in Which the Attorney General Publishes Breach Data125 States and Territories Exempting Entities from the Notification Statute if the Entity is Complying with Other Federal Laws with Notification Requirements (such as HIPAA, GLB, etc.).....126 States and Territories Allowing Flexibility in Notification Requirements to Entities that Maintain Their Own Notification Procedures Consistent with the State Statute127 States and Territories in Which Individuals Have a Private Right of Action.....128 Grading State and Territory Definitions of Personal Information130 Grading State and Territory Notification Deadlines.....132 Grading State and Territory Notification Requirements.....134 Grading State and Territory Enforcement Measures for Violations136
Alaska.....	6	Louisiana.....	46	Oklahoma	82	
Arizona	8	Maine	48	Oregon	84	
Arkansas	10	Maryland	50	Pennsylvania.....	86	
California.....	12	Massachusetts	52	Puerto Rico	88	
Colorado.....	14	Michigan	54	Rhode Island	90	
Connecticut	18	Minnesota	56	South Carolina	92	
Delaware	20	Mississippi	58	South Dakota	94	
District of Columbia.....	22	Missouri	60	Tennessee	96	
Florida	24	Montana	62	Texas	98	
Georgia.....	26	Nebraska	64	U.S. Virgin Islands.....	100	
Guam.....	28	Nevada	66	Utah.....	102	
Hawaii	30	New Hampshire	68	Vermont.....	104	
Idaho	32	New Jersey	70	Virginia	106	
Illinois.....	34	New Mexico	72	Washington	108	
Indiana	38	New York.....	74	West Virginia	110	
Iowa.....	40	North Carolina	76	Wisconsin.....	112	
Kansas	42	North Dakota.....	78	Wyoming.....	114	

Alabama

2018 Ala. Laws No. 396

Definition of Breach

The unauthorized acquisition of data in electronic form containing sensitive personally identifying information. Acquisition occurring over a period of time committed by the same entity constitutes one breach.

Definition of Personally Identifiable Information

“Sensitive personally identifying information” is defined as 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: (l) 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.

Form of Data

Any data stored electronically or digitally on any computer system or other database, including, but not limited to, recordable tapes and other mass storage devices.

Paper Records Covered

No.

Encrypted Data Covered When the Encryption Key Has Been Accessed or Acquired

Yes, if the covered entity knows or has reason to know that the encryption key or security credential that could render the information readable has been breached as well.

Entities Covered

Any person, sole proprietorship, partnership, government entity, corporation, nonprofit, trust, estate, cooperative association, or other business entity that acquires or uses sensitive personally identifying information, or any 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.

Notification Obligation Triggers After Discovery or After Reasonable Investigation

The determination 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.

Time for Notification Once an Obligation is Triggered

If entity owns the data, as expeditiously as possible and without unreasonable delay, within 45 days. If entity licenses or maintains data, 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.

Risk of Harm Trigger for Notification Exists

Yes.

Notification Method

Written and 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. Substitute notice may be provided if direct notice is not feasible due to any of the following factors: (1) Excessive cost to the covered entity relative to the resources of the covered entity; (2) The cost to the entity exceeds \$500,000; (3) Lack of sufficient contact information for the individual required to be notified; (4) More than 100,000 persons must be notified.

Mandatory Notification Items

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; and (5) Information that the individual can use to contact the covered entity to inquire about the breach. If the covered entity is giving substitute notice, the notice must include both of the following: (1) A conspicuous notice on the website of the covered entity, if the covered entity maintains a website, for a period of 30 days; and (2) Notice in print and in broadcast media, including major media in urban and rural areas where the affected individuals reside. An alternative form of substitute notice may be used with the approval of the AG.

If notifying the AG of a breach, notice must 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.

Notification Recipients

Any Alabama resident whose sensitive personally identifying information was, or the covered entity reasonably believes to have been, accessed as a result of the breach.

If more than 1,000 persons must be notified, notice must also be provided to AG as expeditiously as possible and without unreasonable delay within 45 days, and must notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in the Fair Credit Reporting Act, 15 U.S.C. 1681a, of the timing, distribution, and content of the notices without unreasonable delay.

A government entity that acquires and maintains sensitive personally identifying information from a government employer, and which is required to provide notice to any individual under this act, must also notify the employing government entity of any individual to whom the information relates.

Attorney General Publishes Breach Data

No.

Private Right of Action Included

No.

Exception to Notification Obligation Exists if the Entity is Complying with Other Laws (HIPPA, GLB, etc.)

Yes.

Allows Flexibility in Notification Requirements to Entities that Maintain Their Own Notification Procedures Consistent with the Statute

No.

Penalties for Violations

Up to \$500,000 in civil penalties for a covered entity that knowingly engaged in violation of the provisions of this act, and \$5,000 per day for each consecutive day a covered entity fails to take reasonable action to comply with this act.

Definition of Breach

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.

Definition of Personally Identifiable Information

Individual’s first name or first initial and his or her last name in combination with one or more of the following data elements when either the name or the data element is not encrypted or (A) SSN; (B) DL number or state ID number; (C) Account number, card number, or debit card number, combination with any req security code or password that would allow access to an individual’s financial account and (D) passwords, personal ID numbers or other access codes for financial accounts.

Form of Data

Information in any form.

Paper Records Covered

Yes.

Encrypted Data Covered When the Encryption Key Has Been Accessed or Acquired

Yes, if information is encrypted and encryption key has been accessed or acquired.

Entities Covered

Any person doing business, any government agency, or person with more than 10 employees that owns or licenses personal information of an AK resident.

Notification Obligation Triggers After Discovery or After Reasonable Investigation

Discovery or notification of a breach. But disclosure not required if, after an appropriate investigation and after written notification to AK AG, entity “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.”

Time for Notification Once an Obligation is Triggered

In the most expedient time possible and without unreasonable delay.

Risk of Harm Trigger for Notification Exists

Yes, if after investigation, entity determines there is not reasonable likelihood of harm to affected individuals, must notify AG.

Notification Method

(1) Written notice; (2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code; or (3) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed \$150K, or that the affected class of subject persons to be notified exceeds 300,000, 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; (B) Conspicuous posting of the notice on the Web site page of the person or business, if the person or business maintains one; and (C) Notification to major statewide media.

Mandatory Notification Items

No applicable provision.

Notification Recipients

Any affected AK resident. If required to notify more than 1,000 AK residents at a single time, must also notify national consumer reporting agencies of the timing, distribution and content of the notice (not applicable to entities subject to GLB Act).

Attorney General Publishes Breach Data

No.

Private Right of Action Included

No.

Exception to Notification Obligation Exists if the Entity is Complying with Other Laws (HIPPA, GLB, etc.)


No.

Allows Flexibility in Notification Requirements to Entities that Maintain Their Own Notification Procedures Consistent with the Statute

No.

Penalties for Violations

If information collector is not a governmental agency, violation is an unfair or deceptive act or practice, information collector is liable to state for a civil penalty of up to \$500 to each AK resident who was not notified, NTE \$50,000 and damages under Alaska Stat. § 45.50.531 (limited to actual economic damages NTE \$500) and Alaska Stat. § 45.50.537 (limited to actual economic damages).



Arizona

Ariz. Rev. Stat. §18-551, 552.

Definition of Breach

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.

Definition of Personally Identifiable Information

(1) an individual’s user name or email address in combination with a password or security question and answer that allows access to the account; or (2) an individual’s first name or first initial and last name in combination with one or more of the following data elements, when either the name or the element is not encrypted or redacted or secured by any other method rendering the element unreadable or unusable: (a) SSN; (b) DL number or number on a nonoperating ID license, (c) a private key that is unique to an individual and that is used to authenticate or sign an electronic record, (d) financial account number, credit card number, or debit card number in combination with any code or password that would allow access to an individual’s financial account, (e) health insurance ID number, (f) information about an individual’s medical or mental health treatment or diagnosis by a health care professional, (g) passport number, (h), taxpayer ID number or an identity protection personal ID number issued by the IRS, or (i) unique biometric data generated from a measurement or analysis of human body characteristics to authenticate an individual when the individuals access an online account.

Form of Data

Unencrypted, unredacted, and computerized.Ariz. Rev. Stat. §18-551.

Paper Records Covered

No.

Encrypted Data Covered When the Encryption Key Has Been Accessed or Acquired

No.

Entities Covered

Person conducting business in AZ that owns, maintains, or licenses unencrypted and unredacted computerized personal information.

Notification Obligation Triggers After Discovery or After Reasonable Investigation

The determination that there has been a breach, after conducting an investigation pursuant to becoming aware of a security incident.

Time for Notification Once an Obligation is Triggered

Person who owns or licenses the computerized data must notify individuals within 45 days after determining that a breach has occurred. Person who maintains data must notify, as soon as practicable, the owner or licensee of data.

Risk of Harm Trigger for Notification Exists

Yes.

Notification Method

(1) Written notice; (2) Email notice if the notifier has email 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. Substitute notice if notifier demonstrates that notice would exceed \$50K, the affected class would be great than 100,000 persons, or the notifier does not have sufficient contact information, in which case notice shall be given by the following: (A) a written letter to the AG that demonstrates the facts necessary for substitute notice; and (B) Conspicuous posting of the notice on the web site for at least 45 days if a web site is maintained.

Mandatory Notification Items

Notice must contain: (1) the approximate date of the breach, (2) a brief description of the personal information included in the breach, (3) the toll-free numbers and addresses for the 3 largest nationwide consumer reporting agencies, (4) the toll-free number, address, and website address for the FTC or any federal agency that assists consumers with identity theft matters.

Notification Recipients

Any affected AZ resident; data owner, if notifier is not owner.

Attorney General Publishes Breach Data

No.

Private Right of Action Included

No.

Exception to Notification Obligation Exists if the Entity is Complying with Other Laws (HIPPA, GLB, etc.)

Yes, (1) entities regulated by federal or state law that notify in accordance with that federal or state law are exempt. Ariz. Rev. Stat. §18-545(F); (2) entities subject to Title V of GLB Act; (3) covered entities under HIPAA.

Allows Flexibility in Notification Requirements to Entities that Maintain Their Own Notification Procedures Consistent with the Statute

Yes.

Penalties for Violations

AG may impose civil penalties of up to \$10,000 per individual or the total amount of economic loss sustained by affected individuals, but the total may not exceed \$500,000.

Arkansas

Ark. Code Ann. § 4-110-101 et seq.

Definition of Breach

Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person or business.

Definition of Personally Identifiable Information

Individual’s first name or first initial and his or her last name in combination with one or more of the following data elements when either the name or the data element is not encrypted or (A) SSN; (B) DL number or AR ID number; (C) Account number, credit card number, or debit card number, in combination with any req. security code or password that would allow access to an individual’s financial account and (D) medical information (in electronic OR physical form).

Form of Data

Computerized.

Paper Records Covered

No.

Encrypted Data Covered When the Encryption Key Has Been Accessed or Acquired

No.

Entities Covered

Any person or business that acquires, owns, maintains, or licenses computerized data that includes personal information.

Any entity engaged in the business of insurance.

Notification Obligation Triggers After Discovery or After Reasonable Investigation

Discovery or notification that personal information was, or believed to be, acquired. But notification not required if, after a reasonable investigation, the person or business determines that there is no reasonable likelihood of harm to customers.

Time for Notification Once an Obligation is Triggered

If the person or business maintains the computerized data, immediately following the discovery of the breach.

Risk of Harm Trigger for Notification Exists

Yes.

Notification Method

(1) Written notice; (2) Electronic mail notice if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001; or (3) Substitute notice if the person or business demonstrates that the cost of providing notice would exceed \$250K, the affected class would exceed 500,000, or the business or person does not have necessary contact information. Substitute notice shall consist of all of the following: (A) E-mail if the person or business has an e-mail address for the affected person, (B) Conspicuous posting of the notice on the website of the person or business if the person or business maintains a website, and (C) Notification by statewide media.

Mandatory Notification Items

No applicable provision.

Notification Recipients

If data owner or licensee, any affected person.

If an entity engaged in the business of insurance, any affected person and the Arkansas Insurance Commissioner.

Data owner, if not owner or licensee.

Attorney General Publishes Breach Data

No.

Private Right of Action Included

No.

Exception to Notification Obligation Exists if the Entity is Complying with Other Laws (HIPPA, GLB, etc.)

Compliance with state or federal law that provides greater protection to personal information is deemed compliance with this chapter.

Allows Flexibility in Notification Requirements to Entities that Maintain Their Own Notification Procedures Consistent with the Statute

Yes.

Penalties for Violations

Punishable by AG.



California

Cal. Civ. Code §1798.82; Civ. Code §1798.20

Definition of Breach

Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person, business, or agency.

Definition of Personally Identifiable Information

(1) An individual’s first name or first initial and last name in combination with any one or more of the following data elements: (a) SSN; (b) driver’s license number or CA ID card number (c) account number, credit or debit card number, in combination with any required security access code, or password that would permit access to an individual’s account; (d) medical information, (e) health insurance information and (f) information or data collected through the use or operation of an automated license plate recognition system.

(2) 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.

Form of Data

Computerized.

Paper Records Covered

No.

Encrypted Data Covered When the Encryption Key Has Been Accessed or Acquired

Yes, a breach of encrypted data will trigger a notification requirement if the encryption key or a security credential is also acquired by an unauthorized person, and the owner of licensor of personal information has a reasonable belief that the encryption key or security credential could be used to render the encrypted personal information readable or usable.

Entities Covered

Any person or business that conducts business in CA, and that owns or licenses computerized data that includes personal information.

Notification Obligation Triggers After Discovery or After Reasonable Investigation

Discovery or notification of the breach of the security of the system if the information was, or is reasonably believed to have been, acquired by an unauthorized person.

Time for Notification Once an Obligation is Triggered

In the most expedient time possible and without unreasonable delay, immediately if notifying the data owner.

Risk of Harm Trigger for Notification Exists

No.

Notification Method

(1) Written notice; (2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code; (3) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed \$250K, 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) E-mail notice when the person or business has an e-mail address for the subject persons; (B) Conspicuous posting of the notice on the Web site page of the person or business, if the person or business maintains one; (C) Notification to major statewide media and the Office of Privacy Protection within the State and Consumer Services Agency. Breach notification letters must be titled “Notice of Data Breach” and present required information under the following headings: “What Happened,” “What Information Was Involved,” “What We Are Doing,” “What

You Can Do,” and “For More Information.” The title and headings must be clearly and conspicuously displayed using a font size no smaller than 10-point type. S.B. 570 also provides a model breach notification form, which, if used, is deemed to comply with the content requirements for written notification.

Mandatory Notification Items

A security breach notification shall include, at a minimum: (a) name and contact info. of reporting person or business subject to this section; (b) list of the types of personal info. that were or are reasonably believed to have been the subject of a breach; (c) if the info. is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) 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 notification was delayed as a result of a law enforcement investigation, if possible to determine at time notice is provided; (e) general description of breach incident, if possible at time notice is provided; (f) toll-free telephone numbers and addresses of major credit reporting agencies if breach exposed a SSN or driver’s license or CA ID card number; and (g) if person or business was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services at no cost to the affected person for not less than 12 months, along with all information necessary to take advantage of the offer.

At discretion of person or business, security breach notification may also include any of the following: (a) info. re what person or business has done to protect individuals whose info. has been breached; (b) advice on steps that the person whose info. has been breached may take to protect him or herself.

Notification Recipients

Any affected resident of CA, data owner if notifier is not owner.

If required to notify more than 500 CA residents as a result of a single breach of the security systems, shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General (AG). All insurers, insurance producers, and insurance support organizations must provide the insurance commissioner with any notices or information that is submitted to the AG’s office.

Attorney General Publishes Breach Data

Yes: <https://oag.ca.gov/ecrime/databreach/list>.

Private Right of Action Included

Yes.

Exception to Notification Obligation Exists if the Entity is Complying with Other Laws (HIPPA, GLB, etc.)

A covered entity under HIPAA will be deemed to have complied with the notice requirements if it has complied completely with HIPAA.

Allows Flexibility in Notification Requirements to Entities that Maintain Their Own Notification Procedures Consistent with the Statute

“Person or business that maintains its own notification procedure as part of an information security policy that is otherwise consistent with the timing requirements” can notify individuals according to its own policy.

Additional Exceptions

Timing of notification shall be consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system.

Penalties for Violations

Any customer injured by a violation of this title may bring a civil action to recover damages. Statute specifically authorizes injunctions against businesses violating the statute. Class actions are not barred.

Miscellaneous Provisions

Where online account is breached but no other personal information is breached, notification may be given electronically through the online account.

If, however, there has been a breach of email account login credentials, a person or business providing the affected email services may NOT give notice through the breached email account, but must give notice in other way.

Colorado

Colo. Rev. Stat. § 6-1-716

Definition of Breach

Security breach’ means the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a covered entity. Good faith acquisition of personal information by an employee or agent of a covered entity for the covered entity’s business purposes is not a security breach 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.

Definition of Personally Identifiable Information

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: (A) 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.

Form of Data

Computerized.

Paper Records Covered

No.

Encrypted Data Covered When the Encryption Key Has Been Accessed or Acquired

Yes, the breach of encrypted or otherwise secured personal information must be disclosed in accordance with this section if the confidential process, encryption key, or other means to decipher the secured information was also acquired in the security breach or was reasonably believed to have been acquired.

Entities Covered

Covered entity’ means a person, as defined in section 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 in subsection (1)(i) of this section.”

Notification Obligation Triggers After Discovery or After Reasonable Investigation

A covered entity shall, when it becomes aware that a security breach may have occurred, conduct in good faith a prompt investigation to determine the likelihood that personal information has been or will be misused. The covered entity shall give notice to the affected Colorado residents unless the investigation determines that the misuse of information about a Colorado resident has not occurred and is not reasonably likely to occur. ‘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.

Time for Notification Once an Obligation is Triggered

Notice must be made 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 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. Third-party service providers must notify the covered entity of any security breach “in the most expedient time possible, and without unreasonable delay following discovery of a security breach, if misuse of personal information about a Colorado resident occurred or is likely to occur.”

Risk of Harm Trigger for Notification Exists

Yes.

Notification Method

(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 electronic means or the notice provided is consistent with the provisions regarding electronic records and signatures set forth in ... 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 [\$250,000], the affected class of persons to be notified exceeds [250,000] 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.

Mandatory Notification Items

Notice must include information related to the date of the breach, the type of information acquired, the covered entity’s contact information (as well as contact information for consumer reporting agencies and the FTC), and a statement that residents can obtain information about fraud alerts and security freezes from the FTC and CRAs. If the investigation determines that personal information has been misused or is reasonably likely to be misused, the covered entity must also: (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 comply with this section by providing the security breach notification to that e-mail address, but may instead comply with this section by providing notice through other methods, as defined in subsection (1)(f) of 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 covered entity knows the resident customarily accesses the account.

Notification Recipients

A covered entity shall give notice to the affected Colorado residents if the security breach is reasonably believed to have affected 500 or more Colorado residents, the covered entity must notify the 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 a covered entity is required to notify more than 1,000 Colorado residents, the covered entity shall also notify ... all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis ... of the anticipated date of the notification to the residents and the approximate number of residents who are to be notified. Third-party service providers must notify the covered entity of any security breach in the most expedient time possible, and without unreasonable delay following discovery of a security breach, if misuse of personal information about a Colorado resident occurred or is likely to occur.

Attorney General Publishes Breach Data

No.

Private Right of Action Included

No.

Exception to Notification Obligation Exists if the Entity is Complying with Other Laws (HIPPA, GLB, etc.)

Yes, regulated entities that maintain procedures for breach notification pursuant to state or federal law.

Allows Flexibility in Notification Requirements to Entities that Maintain Their Own Notification Procedures Consistent with the Statute

Yes.

Penalties for Violations

The attorney general may bring an action in law or equity to address violations of this section, section 6-1-713, or section 6-1-713.5, and for other relief that may be appropriate to ensure compliance with this section or to recover direct economic damages resulting from a violation, or both. Upon receipt of notice pursuant to subsection (2) of this section, and with either a request from the governor to prosecute a particular case or with the approval of the district attorney with jurisdiction to prosecute cases in the judicial district where a case could be brought, the attorney general has the authority to prosecute any criminal violations of section 18-5.5-102.

Miscellaneous Provisions

A covered entity that is required to provide notice to affected Colorado residents pursuant to this subsection (2) is prohibited from charging the cost of providing such notice to such residents.



More than
11 Billion
Data Records
Breached
in the U.S. since 2005



Connecticut

Conn. Gen. Stat. § 36a-701b

Definition of Breach

Unauthorized access to or acquisition of electronic files, media, databases or computerized data containing personal information.

Definition of Personally Identifiable Information

Individual’s first name or first initial and last name in combination with any one or more of the following: (1) SSN; (2) DL number or state ID card number; or (3) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to the individual’s financial account.

Form of Data

Electronic files, media, databases or computerized data.

Paper Records Covered

No.

Encrypted Data Covered When the Encryption Key Has Been Accessed or Acquired

No.

Entities Covered

Any person conducting business in CT who, in the ordinary course of business, owns, licenses or maintains computerized personal information.

Notification Obligation Triggers After Discovery or After Reasonable Investigation

Discovery of breach. But notification not required if, after an appropriate investigation and consultation with relevant federal, state and local law enforcement agencies, the person reasonably determines that the breach will not likely result in harm to the individuals whose personal information has been acquired and accessed.

Time for Notification Once an Obligation is Triggered

Notice must be provided “no later than ninety days after the discovery of the breach, unless a shorter time is required under federal law.”

Risk of Harm Trigger for Notification Exists

Yes.

Notification Method

(1) Written notice; (2) telephone notice; (3) electronic notice, provided such notice is consistent with the provisions regarding electronic records and signatures set forth in 15 USC 7001; or (4) substitute notice, provided such person demonstrates that the cost of providing notice would exceed \$250K, that the affected class of subject persons to be notified exceeds 500,000 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.

If breach involves SSNs, person/business must provide at least 12 months of appropriate identity theft prevention services and, if applicable, identity theft mitigation services at no cost to CT residents.

Mandatory Notification Items

No applicable provision.

Notification Recipients

Any affected CT resident, data owner if person is not data owner. Must also notify CT AG in accordance with instructions here. All Insurance Dept licensees and registrants must notify the Insurance Commissioner of any information security incident affecting a CT resident within 5 days of identifying the incident.

Attorney General Publishes Breach Data

No.

Private Right of Action Included

No.

Exception to Notification Obligation Exists if the Entity is Complying with Other Laws (HIPPA, GLB, etc.)

Yes. exception for compliance with other federal regulations (including GLB Act), if applicable.

Allows Flexibility in Notification Requirements to Entities that Maintain Their Own Notification Procedures Consistent with the Statute

Yes.

Penalties for Violations

Constitutes unfair trade practice for purposes of Sec. 42-110b of general statutes and shall be enforced by AG.



Delaware

Del. Code Ann. tit. 6 § 12B-101 et seq

Definition of Breach

Unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an individual or commercial entity.

Definition of Personally Identifiable Information

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: (a) SSN; (b) DL number or DE ID card number; or (c) Account number, or credit or debit card number in combination with any code or password that would permit access to the individual’s financial account. Personal information data elements also include: (a) any state or federal ID card number; (b) passport number; (c) a username or email address, in combination with a password or security questions and answer that would permit access to an online account; (d) medical history, medical treatment by a healthcare professional, diagnosis of mental or physical condition by a health care professional, or DNA profile; (e) health insurance policy number, subscriber ID number, or any other unique identifier used by a health insurer to identify the person; (f) unique biometric data generated from measurements or analysis of human body characteristics for authentication purposes; (g) individual taxpayer ID number.

Form of Data

Computerized.

Paper Records Covered

No.

Encrypted Data Covered When the Encryption Key Has Been Accessed or Acquired

Notification is not required if the affected data is encrypted, unless the encryption key is affected as well and the data owner or licensee reasonably believes that the personal information could be rendered readable.

Entities Covered

Any person who conducts business in DE and owns, licenses, or maintains personal information.

Notification Obligation Triggers After Discovery or After Reasonable Investigation

Notification is triggered at the point in time at which the data owner or licensee has sufficient evidence to conclude that a breach of security has occurred.

Time for Notification Once an Obligation is Triggered

If data owner or licensee, without unreasonable delay but not later than 60 days after determination of the breach of security.

Risk of Harm Trigger for Notification Exists

Yes.

Notification Method

(1) Written notice, (2) Telephonic notice; (3) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in § 7001 of Title 15 of the United States Code or if the notifier’s primary means of communication with the resident is by electronic means; or (4) Substitute notice if the individual or commercial entity required to provide notice demonstrates that providing notice will exceed \$75K, the affected class exceeds 100,000 DE residents, or that person or entity does not have sufficient contact information of the affected person. Substitute notice shall include (A) e-mail notice if the individual or commercial entity has e-mail addresses of the affected class, (B) conspicuous posting of the notice on the website if the individual or the commercial entity maintains one, and (C) notice to a major statewide media.

Mandatory Notification Items

No applicable provision.

Notification Recipients

Any affected DE resident, or the owner or licensee of the personal information if notifier is not the owner or licensee. If more than 500 DE residents must be notified, AG must be notified as well.

Attorney General Publishes Breach Data

No.

Private Right of Action Included

No.

Exception to Notification Obligation Exists if the Entity is Complying with Other Laws (HIPPA, GLB, etc.)

Yes.

Allows Flexibility in Notification Requirements to Entities that Maintain Their Own Notification Procedures Consistent with the Statute

Yes, entities regulated by federal or state law (such as HIPAA or GLB Act) that notify in accordance with that federal or state law are exempt.

Penalties for Violations

AG may bring action in law or equity under 29 Del. Code § 2517.

Miscellaneous Provisions

If the affected data is a DE resident’s email account login credentials, notification may not be made through that email account. Notification must be provided in one of the other methods described in Del. Code tit. 6, § 12B-101(3), or through a clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an IP address or online location from which the notifier knows the resident customarily access the account.

Additionally, if the breach involves a resident’s SSN, the notifier must offer to the resident credit monitoring services at no cost to the resident for a period of one year, unless the notifier reasonably determines that the breach is unlikely to result in harm.

District of Columbia

D.C. Code § 28-3851 et seq.

Definition of Breach

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 business.

Definition of Personally Identifiable Information

An individual's first name or first initial and last name, or phone number, or address, and any one or more of the following data elements: (I) SSN; (II) DL number or DC ID card number; (III) credit card number or debit card number; or (ii) any other number or code or combination, of numbers or codes, such as account number, security code, access code, or password, that allows access to or use of, an individual's financial or credit account.

Form of Data

Computerized or electronic.

Paper Records Covered

No.

Encrypted Data Covered When the Encryption Key Has Been Accessed or Acquired

No.

Entities Covered

Any person or entity conducting business in D.C. and, through the course of business, owns, maintains, or licenses computerized or electronic personal information.

Notification Obligation Triggers After Discovery or After Reasonable Investigation

Discovery of breach.

Time for Notification Once an Obligation is Triggered

If data owner or licensee, in the most expedient time possible and without unreasonable delay. If not data owner, in the most expedient time possible.

Risk of Harm Trigger for Notification Exists

No.

Notification Method

(1) Written notice; (2) Electronic notice if the customer has consented to receipt of electronic notice that is consistent with signatures in the Electronic Signatures in Global and National Commerce Act; or (3) Substitute notice allowed if the person or business demonstrates that the cost of providing notice would exceed \$50K, the number of persons affected exceeds 100,000, or the person or business does not have sufficient contact information. Substitute notice shall consist of (A) E-mail notice if the person or business has the subject's e-mail address; (B) Conspicuous posting of the notice on the person or entity's website if a website is maintained; and (C) Notice to a major local and, if applicable, national media.

Mandatory Notification Items

No applicable provision.

Notification Recipients

Any affected D.C. resident, or owner or licensee of the personal data if notifier is not the owner or licensee. If required to notify more than 1,000 DC residents at a single time, must also notify all nationwide consumer reporting agencies of the timing, distribution, and content of notices (not applicable to person or entities subject to GLB Act).

Attorney General Publishes Breach Data

No.

Private Right of Action Included

Yes.

Exception to Notification Obligation Exists if the Entity is Complying with Other Laws (HIPPA, GLB, etc.)

Exception for entities required to comply with GLB notification requirements.

Allows Flexibility in Notification Requirements to Entities that Maintain Their Own Notification Procedures Consistent with the Statute

Yes.

Penalties for Violations

Civil action by affected resident for actual damages and costs, AG may also pursue temporary or permanent injunctive relief and civil penalty not to exceed \$100 per violation per resident and costs.

Definition of Breach

Unauthorized access of data in electronic form containing personal information.

Definition of Personally Identifiable Information

(a) Individual’s first name or first initial and last name, in combination with any one or more of the following data elements if the data elements are not encrypted: (i) SSN; (ii) DL number or ID card number, passport number, military ID number or other similar number issued on a government document used to verify identity; (iii) financial account number, credit card number, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account; (iv) any information regarding an individual’s medical history, mental or physical condition or medical treatment or diagnosis by a health care professional; (v) an individual’s health insurance policy number of subscriber ID number and any unique identifier used by a health insurer to identify the individual; or

(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.

Form of Data

Data stored electronically or digitally on any computer system or other database, including recordable tapes and other mass storage devices.

Paper Records Covered

No.

Encrypted Data Covered When the Encryption Key Has Been Accessed or Acquired

No.

Entities Covered

Sole proprietorships, partnerships, corporations, trusts, estates, cooperatives, associations, or other commercial entities that acquire, maintain, store, or use personal information. For purposes of notice requirements, includes governmental entities.

Notification Obligation Triggers After Discovery or After Reasonable Investigation

Determination of the breach, if a FL resident’s unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Notification not required if, after an appropriate investigation and written consultation with relevant fed and state law enforcement agencies, the covered entity reasonably determines that the breach has not and will not likely result in identity theft or any other financial harm to the individuals whose personal information has been accessed. Such a determination must be in writing and maintained for at least 5 years. Covered entity shall provide the written determination to the Department of Legal Affairs within 30 days.

Time for Notification Once an Obligation is Triggered

As expeditiously as practicable and without unreasonable delay, but no later than 30 days after the determination of a breach. 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.

Third-party agent must notify covered entity of 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; covered entity must then provide required notices.

Risk of Harm Trigger for Notification Exists

Yes.

Notification Method

(1) Written notice sent to the mailing address of the individual in the records of the covered entity; (2) E-mail notice sent to the e-mail address of the individual in the records of the covered entity; or (3) Substitute notice, if direct notice is not feasible because the cost of providing notice would exceed \$250,000, the affected individuals exceed 500,000 persons, or the covered entity does not have an e-mail address or mailing address for the affected individuals. Substitute notice shall include: (a) a conspicuous notice on the Internet website of the covered entity; and (b) notice in print to broadcast media, including major media in urban and rural areas where the affected individuals reside.

Mandatory Notification Items

Written notice to the Department of Legal Affairs must include: (1) synopsis of the events surrounding breach; (2) number of individuals in Florida 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, and instructions as to how to use such services; (4) a copy of the notice sent to the individuals; (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.

Written notice to an individual must 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. Fla. Stat.

Notification Recipients

- (1) Any affected resident of FL.
- (2) If 500 or more individuals in the state are affected, notice to the Department of Legal Affairs must be made within 30 days after the determination of the breach or reason to believe a breach had occurred.
- (3) If required to notify more than 1,000 FL residents at a single time, must also notify all nationwide consumer reporting agencies of the timing, distribution and content of the notices.

Attorney General Publishes Breach Data

No.

Private Right of Action Included

No.

Exception to Notification Obligation Exists if the Entity is Complying with Other Laws (HIPPA, GLB, etc.)

Yes.

Allows Flexibility in Notification Requirements to Entities that Maintain Their Own Notification Procedures Consistent with the Statute

No.

Penalties for Violations

Violation shall constitute an unfair or deceptive trade practice in any action brought by the Department of Legal Affairs.

Civil penalties not to exceed \$500,000: (a) \$1000 per day notice is late up to 30 days, (b) thereafter, \$50,000 per 30-day period or portion thereof, up to 180 days, (c) if violation continues for more than 180 days, up to \$500,000 fine. Civil penalties for failure to notify shall apply per breach and not per affected individual.

Miscellaneous Provisions

Each covered entity or third-party agent must take all reasonable measures to dispose, or arrange for the disposal, of customer records containing personal information within its custody or control when the records are no longer to be retained. Such disposal shall involve shredding, erasing, or otherwise modifying personal information in the records to make it unreadable or undecipherable through any means.



Georgia

Ga. Code § 10-1-912

Definition of Breach

Unauthorized acquisition of an individual’s electronic data that compromises the security, confidentiality, or integrity of personal information of such individual maintained by an information broker or data collector.

Definition of Personally Identifiable Information

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) SSN; (B) DL number or state ID 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 PINs or other access codes; or (E) Any of the items in subparagraphs (A) through (D) of this paragraph 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.

Form of Data

Computerized.

Paper Records Covered

No.

Encrypted Data Covered When the Encryption Key Has Been Accessed or Acquired

No.

Entities Covered

(1) Information brokers and (2) data collectors that maintain computerized data that includes personal information of GA residents.

Notification Obligation Triggers After Discovery or After Reasonable Investigation

Following discovery or notification of a breach.

Time for Notification Once an Obligation is Triggered

If the information broker or data collector maintains computerized data, in the most expedient time possible and without unreasonable delay. If person or business maintains computerized data on behalf of an information broker, within 24 hours following discovery.

Risk of Harm Trigger for Notification Exists

No.

Notification Method

(1) Written notice, (2) Telephone notice; (3) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code; or (4) Substitute notice, if the information broker or data collector demonstrates that the cost of providing notice would exceed \$50,000, the affected class of individuals to be notified exceeds 100,000, or that the information broker or data collector does not have sufficient contact information to provide written or electronic notice to such individuals. Substitute notice shall consist of (A) E-mail notice if the information broker has the individual’s e-mail address, (B) Conspicuous posting of the notice on the information broker’s website if one is maintained, and (C) Notification to major state-wide media.

Mandatory Notification Items

No applicable provision.

Notification Recipients

Any affected resident of GA, or information broker or data collector if notifier is not the owner or licensee. If required to notify more than 10,000 GA residents at a single time, must also notify, w/o unreasonable delay, all national consumer reporting agencies of the timing, distribution and content of the notices.

Attorney General Publishes Breach Data

No.

Private Right of Action Included

No.

Exception to Notification Obligation Exists if the Entity is Complying with Other Laws (HIPPA, GLB, etc.)

No.

Allows Flexibility in Notification Requirements to Entities that Maintain Their Own Notification Procedures Consistent with the Statute

Yes.

Penalties for Violations

No applicable provision.





9 Guam Code Ann. § 48.10 et seq.

Definition of Breach

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.”

Definition of Personally Identifiable Information

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 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. (4) The term 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.

Form of Data

Unencrypted, unredacted, and computerized.

Paper Records Covered

No.

Encrypted Data Covered When the Encryption Key Has Been Accessed or Acquired

No.

Entities Covered

Any individual or entity that owns or licenses computerized data that includes personal information.

Notification Obligation Triggers After Discovery or After Reasonable Investigation

Discovery that a breach has occurred or is reasonably believed to have occurred.

Time for Notification Once an Obligation is Triggered

If data owner, without unreasonable delay. If data licensee, must notify data owner as soon as practicable.

Risk of Harm Trigger for Notification Exists

Yes.

Notification Method

(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 required to provide notice demonstrates that the cost of providing notice will exceed \$10,000, or that the affected class of residents to be notified exceeds 5,000 people, or that the individual or the entity does not have sufficient contact information or consent to provide notice as described in 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.

Mandatory Notification Items

No applicable provision.

Notification Recipients

If data owner, residents of Guam affected by breach. If data licensee, data owner.

Attorney General Publishes Breach Data

No.

Private Right of Action Included

No, the attorney general has exclusive authority to bring action.

Exception to Notification Obligation Exists if the Entity is Complying with Other Laws (HIPPA, GLB, etc.)

Yes, entities that are subject to and in compliance with the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, or with the notification requirements established by the entity’s Federal regulator are deemed in compliance with the notification requirements of Guam.

Allows Flexibility in Notification Requirements to Entities that Maintain Their Own Notification Procedures Consistent with the Statute

Yes.

Penalties for Violations

Actual damages or a civil penalty not to exceed \$150,000 per breach of the security of the system or series of breaches of a similar nature that are discovered in a single investigation.



Definition of Breach

Incident of unauthorized access to and acquisition of unencrypted or unredacted records or data containing personal information where illegal use of personal information has occurred, or is reasonably likely to occur and that creates a risk of harm to a person.

Definition of Personally Identifiable Information

Individual’s first name or first initial and last name in combination with any 1 or more of the following data elements, when either the name or the data elements are not encrypted: (1) SSN; (2) DL number or HI ID 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.

Form of Data

Computerized or unredacted paper records.

Paper Records Covered

Yes.

Encrypted Data Covered When the Encryption Key Has Been Accessed or Acquired

Yes, encrypted records or data containing personal information along with the confidential process or key.

Entities Covered

Any business that owns, maintains, or licenses personal information of Hawaii residents, or any government agency that collects personal information for governmental purposes.

Notification Obligation Triggers After Discovery or After Reasonable Investigation

Following discovery or notification of a security breach.

Time for Notification Once an Obligation is Triggered

If business owns or licenses personal information, without unreasonable delay. “Immediately,” if notifying data owner.

Risk of Harm Trigger for Notification Exists

Yes.

Notification Method

(1) Written notice, (2) Telephonic notice provided that contact is made directly with the affected person; (3) E-mail notice if e-mail is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code; or (4) Substitute notice if the business or government agency demonstrates that the cost of providing notice would exceed \$100,000 or that the affected class of subject persons to be notified exceeds 200,000, or if the business or government agency does not have sufficient contact information or consent, for only those affected persons without sufficient contact information or consent, or if the business or government agency is unable to identify particular affected persons, for only those unidentifiable affected persons. Substitute notice shall consist of all the following Substitute notice shall consist of: (A) E-mail notice when the business or government agency has an e-mail address for the subject persons; (B) Conspicuous posting of the notice on the website page of the business or government agency, if one is maintained; and (C) Notification to major statewide media.

Mandatory Notification Items

Notice shall be “clear and conspicuous.” (1) Description of incident in general terms; (2) Type of personal info subject to unauthorized access/acquisition; (3) General acts of business or agency to protect personal info from further unauthorized access; (4) Phone number that person may call for further info, if one exists, and (5) Advice that directs person to remain vigilant by reviewing account statements and monitoring credit reports.

Notification Recipients

Any affected individual, data owner or licensee if notifier is not owner or licensee. If breach affects more than 1000 persons, must also notify the HI Office of Consumer Protection and national consumer reporting agencies.

Attorney General Publishes Breach Data

No.

Private Right of Action Included

Yes.

Exception to Notification Obligation Exists if the Entity is Complying with Other Laws (HIPPA, GLB, etc.)

Yes, for (1) financial institutions subject to Federal Interagency Guidance on Response Programs for Unauthorized Access to Consumer Information or 12 CFR 748; (2) health care providers or health plans in compliance with HIPAA privacy standards.

Allows Flexibility in Notification Requirements to Entities that Maintain Their Own Notification Procedures Consistent with the Statute

No.

Penalties for Violations

Penalties NTE \$2500 fine for each violation. AG, executive director of the office of consumer protection or any injured party may bring a civil action to recover damages and attorney’s fees. No actions may be brought against a government agency.



Idaho

Idaho Code § 28-51-104 - 107

Definition of Breach

Illegal acquisition of unencrypted computerized data that materially compromises the security, confidentiality, or integrity of personal information for one or more persons maintained by an agency, individual or a commercial entity.

Definition of Personally Identifiable Information

ID resident's first name or first initial and last name in combination with any one or more of the following data elements that relate to the resident, when either the name or the data elements are not encrypted: (a) SSN; (b) DL number or ID card number; (c) Account number, or credit or debit card number, in combination with any code or password that would permit access to a resident's financial account.

Form of Data

Computerized.

Paper Records Covered

No.

Encrypted Data Covered When the Encryption Key Has Been Accessed or Acquired

No.

Entities Covered

A city, county or state agency, individual or a commercial entity that conducts business in Idaho and that owns, maintains, or licenses computerized data that includes personal information about a resident of Idaho.

Notification Obligation Triggers After Discovery or After Reasonable Investigation

Discovery or notification of the breach, following an investigation of whether harm has occurred.

Time for Notification Once an Obligation is Triggered

“[I]n the most expedient time possible and without unreasonable delay,” if data owner/licensee.

“Immediately,” if data is only maintained and need to notify data owner/licensee.

Risk of Harm Trigger for Notification Exists

Yes.

Notification Method

(1) Written notice to the most recent address the agency, individual or commercial entity has in its records; (2) Telephonic notice; (3) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. section 7001; or (4) Substitute notice, if the agency, individual or the commercial entity required to provide notice demonstrates that the cost of providing notice will exceed \$25,000, or that the number of Idaho residents to be notified exceeds 50,000, or that the agency, individual or the commercial entity does not have sufficient contact information to provide notice. Substitute notice consists of all of the following: (a) E-mail notice if the agency, individual or the commercial entity has e-mail addresses for the affected Idaho residents; (ii) Conspicuous posting of the notice on the website page of the agency, individual or the commercial entity, if one is maintained; and (iii) Notice to major statewide media.

Mandatory Notification Items

No applicable provision.

Notification Recipients

Affected resident, or owner or licensee of the information if notifier is not the owner or licensee. If an agency becomes aware of a breach, must notify ID AG within 24 hours of discovery.

Attorney General Publishes Breach Data

No.

Private Right of Action Included

No.

Exception to Notification Obligation Exists if the Entity is Complying with Other Laws (HIPPA, GLB, etc.)

Yes, entities regulated by federal or state law that notify in accordance with that federal or state law are exempt.

Allows Flexibility in Notification Requirements to Entities that Maintain Their Own Notification Procedures Consistent with the Statute

Yes.

Penalties for Violations

Civil action by regulating agency; Fine NTE \$25,000 per breach if failure to notify is intentional.



815 Ill. Compt. Stat. §§ 530/1–530/50

Definition of Breach

Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the data collector.

Definition of Personally Identifiable Information

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 through a breach of security: (1) SSN; (2) driver’s license number or state ID card number; (3) Account number or credit or debit card number, or an account number or credit card number in combination with any required code or password that would permit access to an individual’s financial account; (4) Medical information; (5) Health insurance information; or (6) 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.

Personal information may also include a 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.

Form of Data

Computerized.

Paper Records Covered

No.

Encrypted Data Covered When the Encryption Key Has Been Accessed or Acquired

Yes, if breach involves encrypted or redacted data along with the keys needed to unencrypt, unredact, or otherwise read the name or data elements, notification is required.

Entities Covered

Any government agencies, public and private universities, privately and publicly held corporations, financial institutions, retail operators, and any other entity that, for any purpose, handles, collects, disseminates, or otherwise deals with nonpublic personal information.

Notification Obligation Triggers After Discovery or After Reasonable Investigation

For any data collector that owns or licenses personal information: “following discovery or notification of the breach”.

For any data collector that maintains or stores, but does not own or license, computerized data: “following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.”

Time for Notification Once an Obligation is Triggered

If owns or licenses personal information, “without unreasonable delay, in the most expedient time possible.”

If data collector maintains personal information, “immediately” following discovery.

Risk of Harm Trigger for Notification Exists

No.

Notification Method

(1) Written notice; (2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code; or (3) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed \$250K, or that the affected class of subject persons to be notified exceeds 500,000, or that the data collector does not have sufficient contact information. Substitute notice shall consist of (A) E-mail notice if the data collector has the email addresses to the affected persons; (B) Conspicuous posting of the notice on the data collector’s website if one is maintained; and (C) Notification to major statewide media. If breach impacts residents in one geographic area, notification to media may be made to prominent local media in areas where affected individuals are likely to reside if such notice is reasonably calculated to give actual notice to persons whom notice is required.

Mandatory Notification Items

Disclosure to an IL resident shall include, but need not be limited to, (i) the toll-free numbers and addresses for consumer reporting agencies, (ii) the toll-free number, address and website address for the FTC, and (iii) a statement that the individual can obtain information from these sources about fraud alerts and security freezes. Notification shall not include information concerning the number of IL residents affected by the breach.

If compromised data is a user name or email address, in combination with password or security question and answer that would permit access to an online account, notice may be provided in electronic or other form directing the IL resident to change his/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.

When informing data owner, entity must “cooperate with the owner or licensee,” which shall include, but need not be limited to, (i) informing the owner or licensee of the breach, including giving notice of the date or approx. date of the breach and the nature of the breach, and (ii) informing the owner or licensee of any steps the data collector has taken or plans to take relating to the breach.

Notification Recipients

Any affected resident, data owner or licensee if notifier is not owner or licensee. If State agency required to notify more than 1,000 persons, it must also notify, without unreasonable delay, all national consumer reporting agencies.

If State agency required to notify more than 250 IL residents, must notify AG within 45 days of discovery of breach or when the State agency notifies individuals affected by breach, whichever is sooner. Further instructions for notifying AG can be found here. Notice to AG must include (A) types of personal information compromised in breach; (B) number of IL residents affected by the breach at the time of notification; (C) any steps the State agency has taken or plans to take relating to notification of the breach to consumers; and (D) date and timeframe of the breach, if known at the time of notification (if not known at the time of notification, must send to AG as soon as possible).

If the State agency that suffers breach determines the identity of the actor who perpetrated the breach, the State agency must notify the General Assembly within 5 days after the determination, provided that the disclosure would not jeopardize the security of IL residents or compromise a security investigation.

If a State agency directly responsible to the Governor has been or has reason to believe it has been subject to a data breach of more than 250 IL residents, must notify Office of the Chief Information Security Officer of the Illinois Department of Innovation and Technology and AG no later than 72 hours following discovery of the breach.

Attorney General Publishes Breach Data

No.

Private Right of Action Included

No.

Exception to Notification Obligation Exists if the Entity is Complying with Other Laws (HIPPA, GLB, etc.)

Yes if: (1) the entity complies with state or federal laws that provide greater protection to personal information than this section; (2) the entity is subject to and in compliance with standards established by §501(b) of GLB Act; or (3) the entity is subject to and in compliance with the privacy and security standards for the protection of electronic health information set by HIPAA.

Allows Flexibility in Notification Requirements to Entities that Maintain Their Own Notification Procedures Consistent with the Statute

Yes.

Penalties for Violations

Violation of the Consumer Fraud and Deceptive Business Practices Act. Any person who improperly disposes of materials containing personal information is subject to a civil penalty of not more than \$100 for each individual with respect to whom personal information is disposed of, NTE \$50,000 for each instance of improper disposal of materials containing personal information. As amended, Attorney General may file a civil action to recover any penalty imposed for improper disposal or to seek any appropriate relief.

Miscellaneous Provisions

A person (including a natural person, a corporation, partnership, association or other legal entity, unit of local government or any agency, department, division, bureau, board, commission or committee thereof; or the State of IL or any constitutional officer, agency, department, division, bureau, board, commission or committee thereof) must dispose of the materials containing personal information in a manner that renders the personal information unreadable, unusable and undecipherable.

Majority of
Americans
have **Personally**
Experienced
a **Major Data**
Breach



Indiana

Ind. Code § 24-4.9-1-1 et. Seq

Definition of Breach

Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information.

Definition of Personally Identifiable Information

If notifier is not a state or local agency: (1) a SSN that is not encrypted or redacted; or (2) an individual’s first and last names, or first initial and last name, and one or more of the following data elements that are not encrypted or redacted: (A) DL number; (B) state ID card number; (C) credit card number; or (D) a financial account number or debit card number in combination with a code or password that would permit access to the person’s account.

If notifier is a state or local agency: (1) an individual’s: (A) first name and last name; or (B) first initial and last name; and (2) at least one of the following data elements: (A) SSN; (B) DL number or state ID card number. (C) Account number, credit card number, debit card number, security code, access code, or password of an individual’s financial account.

Form of Data

Computerized.

Paper Records Covered

No.

Encrypted Data Covered When the Encryption Key Has Been Accessed or Acquired

Yes, if notifier is not a state or local agency and encrypted personal information was or may have been acquired by an unauthorized person with access to the encryption key. No, if notifier is a state or local agency.

Entities Covered

An individual, a corporation, a business trust, an estate, a trust, a partnership, an association, a nonprofit corporation or organization, a cooperative, or any other legal entity that owns or licenses computerized data that includes personal information.

A state agency that owns or licenses computerized data that includes personal information.

Notification Obligation Triggers After Discovery or After Reasonable Investigation

After discovering or being notified of a breach, but only required to notify if 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 IN resident.

Time for Notification Once an Obligation is Triggered

Without unreasonable delay.

Risk of Harm Trigger for Notification Exists

Yes.

Notification Method

If notifier is not a state or local agency: (1) Mail; (2) Telephone; (3) Fax; (4) E-mail (if e-mail address is known); or (4) Substitute notice permitted if must be made to more than 500,000 IN residents or data base owner determines that cost of providing notice exceeds \$250K. Substitute notice shall consist of (A) Conspicuous posting of the notice on the website if one is maintained and (B) Notice to major news reporting media in the geographic area where the IN residents affected reside.

If notifier is a state or local agency: (1) in writing; (2) by electronic mail, if the individual has provided the state agency with the individual’s electronic mail address;

or (3) substitute notice, if notification must be made to more than 500,000 IN residents, cost of providing notice exceeds \$250K, or agency does not have sufficeint contact information. Substitute notice may consist of (A) Conspicuous posting of the notice on the website if one is maintained and (B) Notice to major news reporting media in the geographic area where the IN residents affected reside.

Mandatory Notification Items

No applicable provision.

Notification Recipients

If notifier is not a state or local agency: All affected IN residents, as well as AG. If required to notify more than 1,000 IN residents at a single time, must also notify national consumer reporting agencies of the distribution and content of the notice. Data base owner if notifier is not owner. If notifier is a state or local agency: All affected IN residents. Data base owner if notifier is not owner.

All “Navigators” (i.e. individuals assisting consumers complete health coverage applications) must notify the Dept of Insurance within 5 days of discovery of a security breach.

Attorney General Publishes Breach Data

No.

Private Right of Action Included

No.

Exception to Notification Obligation Exists if the Entity is Complying with Other Laws (HIPPA, GLB, etc.)

Entities in compliance with certain federal laws (including GLB Act, HIPAA) and financial institutions that comply with Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information, etc. are exempt. No applicable provision for state and local agencies.

Allows Flexibility in Notification Requirements to Entities that Maintain Their Own Notification Procedures Consistent with the Statute

Yes, so long as policy is as stringent as several of IN requirements. No applicable provision for state and local agencies.

Additional Exceptions

Theft of password-protected portable devices does not violate the statute, if all personal info on device is protected by encryption and encryption key has not been compromised or disclosed & is not in possession of, or known to the person who, without authorization, acquired or has access to the portable electronic device.

Penalties for Violations

If notifier is not a state or local agency: failure to notify as required results in a “deceptive act” that is actionable only by the AG. Failure to make a required notification in connection with a related series of breaches of the security of data constitutes one deceptive act. AG may bring an action for any or all of the following: (1) an injunction; (2) civil penalty NTE \$150,000 per deceptive act; and (3) AG’s reasonable costs in the investigation of the deceptive act and maintaining the action.

No applicable provision for state or local agencies.

Miscellaneous Provisions

If notifier is not a state or local agency: Includes the unauthorized acquisition of computerized data that have been transferred to another medium, including paper, microfilm, or a similar medium, even if the transferred data are no longer in a computerized format. Unauthorized acquisition of a personal electronic device on which personal information is stored does not trigger breach notification requirements if all personal information on device is encrypted and the encryption key (A) has not been compromised or disclosed; and (B) is not in the possession of or known to the person with unauthorized access to the device.

If notifier is a state or local agency, unauthorized acquisition of a portable electronic device on which personal information is stored does not trigger breach notification requirements if access to the device is protected by a password that has not been disclosed.

1

Kansas

Kan. Stat. § 50-7a01 et seq

Definition of Breach

“[U]nauthorized 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.”

Definition of Personally Identifiable Information

Consumer’s first name or first initial and last name linked to any one or more of the following data elements that relate to the consumer, when the data elements are neither encrypted nor redacted: (1) SSN; (2) DL number or state ID card number; or (3) financial account number, or credit or debit account number, alone or in combination with any required code or password that would permit access to a consumer’s financial account.

Form of Data

Computerized.

Paper Records Covered

No.

Encrypted Data Covered When the Encryption Key Has Been Accessed or Acquired

No.

Entities Covered

Any person that conducts business in KS, or a government agency, governmental subdivision or agency that owns, licenses, or maintains computerized data.

Notification Obligation Triggers After Discovery or After Reasonable Investigation

Following a “reasonable and prompt investigation” to determine the likelihood that personal information has been or will be misused.

Time for Notification Once an Obligation is Triggered

If person owns or licenses of the personal data, “in the most expedient time possible and without unreasonable delay.” If the individual or commercial entity maintains personal data, must notify data owner “following discovery of a breach.”

Risk of Harm Trigger for Notification Exists

Yes.

Notification Method

(1) Written notice; (2) E-mail notice if notice is consistent the provisions regarding electronic records and signatures in 15 U.S.C. § 7001; or (3) Substitute notice, if individual or commercial entity demonstrates that the cost of providing notice would exceed \$100K, affected class of consumers exceeds 5,000, or individual or commercial entity does not have sufficient contact information. Substitute notice shall consist of (A) e-mail if individual or entity has obtained e-mail address; (B) conspicuous posting of the notice on web site, if individual or entity maintains a web site; and (C) notification to major statewide media.

Mandatory Notification Items

No applicable provision.

Notification Recipients

If person or government entity owns or licenses personal information, then notification is to affected KS resident. If individual or commercial entity only maintains personal information, then notification is to the owner or licensee of the information. But if required to notify more than 1,000 individuals at a single time, must also notify national consumer reporting agencies of the timing, distribution, and content of the notices.

Attorney General Publishes Breach Data

No.

Private Right of Action Included

No.

Exception to Notification Obligation Exists if the Entity is Complying with Other Laws (HIPPA, GLB, etc.)

Regulated entities subject to state or federal law and that maintain procedures for a breach of the security of the system pursuant to laws, rules, regulations, guidance or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance.

Allows Flexibility in Notification Requirements to Entities that Maintain Their Own Notification Procedures Consistent with the Statute

Yes.

Penalties for Violations

AG allowed to bring action in law or equity, except as to insurance companies (insurance commissioner has sole authority to bring action against insurance companies).



Definition of Breach

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 re multiple individuals that actually causes, or leads the information holder to reasonably believe has caused or will cause, identity theft or fraud against any KY resident.

Definition of Personally Identifiable Information

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 data element is not redacted: (1) SSN; (2) Driver’s license number; or (3) Account number, credit or debit card number, in combination with any required security code, access code or password permitting access to an individual’s financial account.

Form of Data

Computerized.

Paper Records Covered

No.

Encrypted Data Covered When the Encryption Key Has Been Accessed or Acquired

No.

Entities Covered

Any person or business entity that conducts business in this state.

Notification Obligation Triggers After Discovery or After Reasonable Investigation

Information holder discovers or is notified of any breach of the security system.

Time for Notification Once an Obligation is Triggered

“[I]n the most expedient time possible and without unreasonable delay” and “as soon as reasonably practicable following discovery,” if notifying data owner or licensee of info.

Risk of Harm Trigger for Notification Exists

Yes. Breach must have actually caused or lead the information holder to reasonably believe that it has caused or will cause, identity theft or fraud against any KY resident.

Notification Method

(1) Written notice; (2) E-mail notice if notice is consistent the provisions regarding electronic records and signatures in 15 U.S.C. § 7001; or (3) Substitute notice, if information holder demonstrates that cost of providing notice would exceed \$250K, affected class of consumers exceeds 500,000, or information holder does not have sufficient contact information. Substitute notice shall consist of (A) E-mail, when information holder has e-mail address for subject persons; (B) Conspicuous posting of notice on information holder’s Internet Web site page, if information holder maintains a Web site page; and (C) Notification to major statewide media.

Mandatory Notification Items

No applicable provision.

Notification Recipients

Any KY resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Ky. Rev. Stat. § 365.732(2).

If notifying more than 1,000 persons at one time, person shall also notify, without unreasonable delay, all nationwide consumer reporting agencies and credit bureaus (as defined by 15 U.S.C. sec. 1681a), of the timing, distribution and content of the notices.

Attorney General Publishes Breach Data

No.

Private Right of Action Included

No applicable provision.

Exception to Notification Obligation Exists if the Entity is Complying with Other Laws (HIPPA, GLB, etc.)

Shall not apply to any person who is subject to GLBA or HIPAA, or any agency of KY or any of its local governments or political subdivisions.

Allows Flexibility in Notification Requirements to Entities that Maintain Their Own Notification Procedures Consistent with the Statute

Yes.

Additional Exceptions

Timing of notification shall be given consistent with the legitimate needs of law enforcement or measures necessary to determine the scope of breach and restore data system.

Penalties for Violations

No applicable provision.

Louisiana

La. Rev. Stat. §§ 51:3071 – 3077

Definition of Breach

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.

Definition of Personally Identifiable Information

Individual’s first name or first initial and last name in combination with any one or more of the following data elements when either the name or the data elements are not encrypted or redacted: (i) SSN; (ii) DL number or state ID number; (iii) account number, credit or debit card number, in combination with any required code or password that would permit access to an individual’s financial account; (iv) passport number; or (v) biometric data.

Form of Data

Computerized.

Paper Records Covered

No.

Encrypted Data Covered When the Encryption Key Has Been Accessed or Acquired

No.

Entities Covered

Any person that owns or licenses, or maintains computerized data that includes personal information of a resident of LA.

Notification Obligation Triggers After Discovery or After Reasonable Investigation

Notification is not required if after a reasonable investigation, the person or business determines that there is no reasonable likelihood of harm to the residents of this state. The person or business shall retain a copy of the written determination and supporting documentation for 5 years from the date of discovery of the breach.

Time for Notification Once an Obligation is Triggered

In the most expedient time possible and without unreasonable delay but not later than sixty days from the discovery of the breach.

Risk of Harm Trigger for Notification Exists

Yes.

Notification Method

1) Written notice; (2) Electronic notification, if notice is consistent the provisions regarding electronic records and signatures in 15 U.S.C. § 7001; or (3) Substitute notice, if agency or person demonstrates that cost of providing notice would exceed \$100K, affected class of consumers exceeds 100,000, or agency or person does not have sufficient contact information. Substitute notice shall consist of (A) E-mail, when agency or person has e-mail address for subject persons; (B) Conspicuous posting of notice on agency or person’s Internet site, if Internet site is maintained; and (C) Notification to major statewide media.

Mandatory Notification Items

No applicable provision.

Notification Recipients

Any affected resident of the state, or owner or licensee if notifier is not the owner or licensee. Also written notice to the Consumer Protection Section of the Attorney General’s Office.

Attorney General Publishes Breach Data

No.

Private Right of Action Included

Yes.

Exception to Notification Obligation Exists if the Entity is Complying with Other Laws (HIPPA, GLB, etc.)

Yes, financial institution that is subject to and in compliance w/ the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice shall be deemed to be in compliance.

Allows Flexibility in Notification Requirements to Entities that Maintain Their Own Notification Procedures Consistent with the Statute

Yes.

Penalties for Violations

May bring civil action to recover actual damages resulting from failure to disclose breach in timely manner.



Me. Rev. Stat. Tit. 10 §§ 1346 – 1350-B

Definition of Breach

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.

Definition of Personally Identifiable Information

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 redacted or encrypted: (A) SSN; (B) DL number or state ID card number; (C) Account number, credit or debit card number, if the number can be used without additional info such as a password or PIN; (D) Account passwords, PINs, or other access codes; or (E) any element in (A)- (D) when not connected to the individual's first name or first initial, and last name, if the information would be sufficient to permit a person to compromise the identity of the person whose information was compromised.

Form of Data

Computerized.

Paper Records Covered

No.

Encrypted Data Covered When the Encryption Key Has Been Accessed or Acquired

No.

Entities Covered

Any individual or entity that maintains computerized data that includes personal information.

Also applies to Information Brokers, which is defined as individual or entity that, for monetary fees or dues, engages in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring or communicating information re individuals for the primary purpose of furnishing personal information to nonaffiliated 3rd parties.

Notification Obligation Triggers After Discovery or After Reasonable Investigation

When person "becomes aware" of a breach, must conduct "a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused." For Information Broker, must notify when, after investigation, the entity finds that personal information of ME resident has been/ reasonably believed to have been, acquired by an unauthorized person. For any other individual or entity, must notify when, after investigation, individual or entity finds that misuse of personal information has occurred/ reasonably possible that misuse will occur.

Time for Notification Once an Obligation is Triggered

As expediently as possible and without unreasonable delay. Immediately, if notifying data owner. If notice delayed for law enforcement purposes, notice must be given within seven business days after a law enforcement agency determines that notification will not compromise a criminal investigation.

Risk of Harm Trigger for Notification Exists

Yes, but for Information Broker must notify, if it finds that personal information has been/reasonably believed to have been acquired; any other individual or entity must notify if it finds that misuse has occurred/reasonably possible that it will occur.

Notification Method

(1) Written notice; (2) Electronic notification if notice is consistent the provisions regarding electronic records and signatures in 15 U.S.C. § 7001; or (3) Substitute notice, if person maintaining personal information demonstrates that the cost of providing notice would exceed \$5K, the affected class of consumers exceeds 1,000, or person does not have sufficient contact information. Substitute notice shall consist of (A) e-mail, if person has e-mail addresses for affected individuals; (B) conspicuous posting of the notice on person's website, if one is maintained; and (C) notification to major statewide media.

Mandatory Notification Items

Notice sent to consumer reporting agencies must include the date of the breach, an estimate of the number of persons affected by the breach, if known, and the actual or anticipated date that persons were or will be notified of the breach.

Notification Recipients

Any affected ME resident. For an individual or entity that must notify affected individuals, must also notify Department of Professional and Financial Regulation, if regulated by the Department. If not, must notify AG. If notifying more than 1,000 people at the same time, must also notify national consumer reporting agencies (include date of breach, estimate of number of persons affected by breach, if known, and actual or anticipated date that persons were or will be notified of breach). All entities licensed by the superintendent are required to notify the superintendent of breaches requiring notice. This notice must include a description of the breach; the number of affected ME residents; a copy of the information sent to affected persons; a description of curative steps; and the name and contact information for a contact person.

Attorney General Publishes Breach Data

No.

Private Right of Action Included

No.

Exception to Notification Obligation Exists if the Entity is Complying with Other Laws (HIPPA, GLB, etc.)

Yes, person that complies with federal/state security breach notification requirements that are at least as protective as notification requirements of this section are deemed to be in compliance with this section.

Allows Flexibility in Notification Requirements to Entities that Maintain Their Own Notification Procedures Consistent with the Statute

No.

Penalties for Violations

Dept of Prof. and Financial Regulation or AG shall enforce. Penalties include one or more of: (1) a fine of not more than \$500 per violation, up to a maximum of \$2,500 for each day the broker is in violation; (2) Equitable relief; (3) Enjoinment from further violations.

Maryland

Md. Code Ann., Com. Law §§ 14-3501 - 3508

Definition of Breach

Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of the personal information maintained by a business.

Definition of Personally Identifiable Information

Personal information” is defined as:

(I) An individual’s first name or first initial and last name in combination with any one or more of the following data elements: (1) SSN, taxpayer ID number, passport number, or other ID number issued by the federal government; (2) DL or state ID card number; (3) account number or credit/debit card number, in combination with any required security/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) health insurance policy or certificate number or health insurance subscriber ID number, in combination with a unique identifier used by an insurer or an employer that it self-insured, that permits access to an individuals’ health information; or (6) biometric data, or (II) A user name or email address in combination with a password or security question and answer that permits access to an individual’s email account.

Form of Data

Computerized.

Paper Records Covered

No.

Encrypted Data Covered When the Encryption Key Has Been Accessed or Acquired

No.

Entities Covered

A business that owns, licenses or maintains computerized data that includes personal information of an individual residing in MD.

Notification Obligation Triggers After Discovery or After Reasonable Investigation

When aware of a breach must conduct “reasonable and prompt” investigation; if investigation reveals likelihood of harm, must notify resident. If only maintaining data, must notify data owner/licensee.

Time for Notification Once an Obligation is Triggered

Notification must be made as soon as is reasonably practicable, but not later than 45 days after investigation.

Risk of Harm Trigger for Notification Exists

Yes, if after investigation, entity determines personal information has not been/ is not likely to be misused, must retain documentation for 3 years.

Notification Method

(1) Written notice; (2) E-mail, provided that individual has expressly consented to receive electronic notice or business conducts its business primarily through Internet account transactions or the Internet; (3) Telephonic notice; or (4) Substitute notice, if business demonstrates that the cost of providing notice would exceed \$100K or that the affected class of individuals to be notified exceeds 175,000 or business does not have sufficient contact information to give notice. Substitute notice shall consist of: (1) E-mailing the notice to an individual, if the business has an individual’s e-mail address and in accordance with requirements for e-mail notice above; (2) Conspicuous posting of the notice on the Web site of the business, if the business maintains a Web site; and (3) Notification to statewide media. In the case of a breach where data allowing unauthorized access to a person’s email account, but no other personal information, is compromised, notice may be provided electronically, directing data subjects to change their passwords or security questions, or take other steps appropriate to protect the email account and all other online accounts for which the data subject uses the same information. The notice may not be sent by email to the same email account affected by the breach, unless the email is access from the same IP address or location that the data subject customarily uses.

Mandatory Notification Items

(1) Description of categories of information breached, including elements of personal information believed to have been breached; (2) Contact information for the business making the notification, including address, phone number, and toll-free phone number if one is maintained; (3) Toll-free numbers and addresses for major consumer reporting agencies; and (4) toll-free phone numbers, addresses, and website addresses for the FTC and office of the AG, and a statement that an individual can get information from these sources about steps to take to prevent ID theft.

Notification Recipients

Affected individuals (MD residents), or owner or licensee if notifier is not owner or licensee of personal data. Must notify Office of AG prior to notifying individuals and consumer reporting agencies. If more than 1,000 individuals affected, must also notify national consumer reporting agencies of the timing, distribution, and content of the notices.

Attorney General Publishes Breach Data

Yes: <http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/breachnotices.aspx>.

Private Right of Action Included

Yes (under Consumer Protection Act).

Exception to Notification Obligation Exists if the Entity is Complying with Other Laws (HIPPA, GLB, etc.)

Yes, (1) businesses complying with requirements for notification, protection of personal information or destruction of personal information under regulations prescribed by the primary state or federal regulators of the business deemed in compliance, (2) businesses subject to and in compliance with GLB Act & Interagency Guidelines for Security Standards and Response Programs for Unauthorized Access to Personal Information also deemed to be in compliance.

Businesses and affiliates that are subject to and in compliance with HIPAA or HITECH are deemed to be in compliance with this Act.

Allows Flexibility in Notification Requirements to Entities that Maintain Their Own Notification Procedures Consistent with the Statute

No.

Penalties for Violations

Violation of statute is considered an unfair or deceptive trade practice under Md. Com. Law § 13-301. AG may pursue an action, along with private individuals harmed by violation of statute.

Massachusetts

Mass. Gen. Laws ch. 93 H, §§ 1–6

Mass. Gen. Laws Ann. ch. 93A, § 4

Definition of Breach

Unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a MA resident.

Definition of Personally Identifiable Information

An individual’s first name or first initial and last name in combination with any one or more of the following data elements: (1) SSN; (2) DL number or state ID card number; (3) financial account number, credit or debit card number, with or without a security code, access code, or password that would permit access to an individual’s financial account.

Form of Data

Unencrypted, or encrypted and the encryption key.

Paper Records Covered

No.

Encrypted Data Covered When the Encryption Key Has Been Accessed or Acquired

Yes, unauthorized acquisition or use of encrypted electronic data and confidential process or key is capable of compromising the security, confidentiality or integrity of personal information.

Entities Covered

Person or state agency that owns, licenses, or maintains data that includes personal information about a resident in MA.

Notification Obligation Triggers After Discovery or After Reasonable Investigation

When person or agency knows or has reason to know of a breach of security or when the person knows or has reason to know that the personal information of a MA resident was acquired or used by an unauthorized person or used for an unauthorized purpose.

Time for Notification Once an Obligation is Triggered

As soon as practicable and without unreasonable delay.

Risk of Harm Trigger for Notification Exists

Yes, per definition of breach must create a substantial risk of identity theft or fraud against a MA resident.

Notification Method

(1) Written notice; (2) Electronic notice, if notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001(c); and Mass. Gen. Laws § 110G; or

(iii) Substitute notice, if the person or agency required to provide notice demonstrates that the cost of providing written notice will exceed \$250K, or that the affected class of Massachusetts residents to be notified exceeds 500,000 residents, or that the person or agency does not have sufficient contact information to provide notice. Substitute Notice shall consist of all of the following: (i) e-mail notice, if person or agency has e-mail addresses for the members of the affected class of MA residents; (ii) clear and conspicuous posting of the notice on the home page of the person or agency if the person or agency maintains a website; and (iii) publication in or broadcast through media or medium that provides notice throughout MA.

Mandatory Notification Items

Notice shall include consumer’s right to obtain a police report, how a consumer requests a security freeze and the necessary information to be provided when requesting the security freeze, and any fees required to be paid to any of the consumer reporting agencies. Notice shall not include nature of breach or unauthorized acquisition or use or the number of residents of the commonwealth affected by said breach or unauthorized access or use.

Sample notification letter to individuals.

Notice to AG and Office of Consumer Affairs and Business Regulation shall consist of: any steps the person or agency has taken or plans to take relating to the breach pursuant to the applicable federal law, rule, regulation, guidance or guidelines.

Sample notification letter to AG.

OCABR notification portal.

Notification Recipients

If person or agency owns or licenses data, must notify any affected MA resident, AG and Office of Consumer Affairs and Business Regulation (OCABR). Notification of OCABR can be made through online portal. If only maintaining data, must notify data owner or licensee. .

Attorney General Publishes Breach Data

Yes: <http://www.mass.gov/ocabr/data-privacy-and-security/data/data-breach-notification-reports.html>.

Private Right of Action Included

No.

Exception to Notification Obligation Exists if the Entity is Complying with Other Laws (HIPPA, GLB, etc.)

Yes. Person who maintains procedures for responding to a security breach pursuant to federal laws, rules, regulations, guidance or guidelines, is deemed to be in compliance with this chapter if person notifies affected MA residents in accordance with the maintained or required procedures when a breach occurs, provided that person notifies Attorney General and Director of Consumer Affairs and Business Regulation of breach as soon as practical.

Allows Flexibility in Notification Requirements to Entities that Maintain Their Own Notification Procedures Consistent with the Statute

No.

Penalties for Violations

AG may bring an action.

Michigan

Mich. Comp. Laws §§ 445.61, 445.63, 445.65, 445.72

Definition of Breach

Unauthorized access and acquisition of data that compromises the security or confidentiality of personal information maintained by a person or agency as part of a database of personal information regarding multiple individuals.

Definition of Personally Identifiable Information

An individual’s first name or first initial and last name in combination with any one or more of the following data elements: (1) SSN; (2) DL number or state ID card number; (3) demand deposit or other financial account number, credit or debit card number, in combination with required security code, access code or password that would permit access to an individual’s financial account.

Form of Data

Computerized.

Paper Records Covered

No.

Encrypted Data Covered When the Encryption Key Has Been Accessed or Acquired

Yes, if encrypted information was accessed by a person with unauthorized access to the encryption key.

Entities Covered

Person or agency that owns, licenses, or maintains data included in a database.

Notification Obligation Triggers After Discovery or After Reasonable Investigation

Discovery or notification of security breach, except notification not required if 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 MI residents.

Time for Notification Once an Obligation is Triggered

Without unreasonable delay.

Risk of Harm Trigger for Notification Exists

Yes. Notification not required if 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 MI residents.

Notification Method

(1) Written notice, (2) Electronic notice, if any of the following conditions are met: (a) recipient has expressly consented to receive electronic notice; (b) person or agency has an existing business relationship with the recipient that includes periodic e-mail communications and based on those communications the person or agency reasonably believes that it has the recipient’s current e-mail address; or (c) the person or agency conducts its business primarily through internet account transactions or on the internet; (3) Telephonic notice, if (a) notice is not given in whole or in part by use of a recorded message; (b) recipient has expressly consented to receive notice by telephone, or if no consent, the person or agency also provides written or electronic notice if the telephonic notice does not result in a live conversation within 3 business days after the initial attempt to provide telephonic notice; and (4) Substitute notice if person or agency demonstrates that notice will exceed \$250K or affected class will exceed more than 500,000 residents. Substitute notice shall consist of (A) e-mail if person has an e-mail address of the affected person, (B) conspicuous posting of the notice or link to the notice if a website is maintained, and (C) notification to major statewide media.

Mandatory Notification Items

Written/electronic notice must be “clear and conspicuous.” Telephonic notice must “clearly communicate the content to the recipient of the telephone call.” All notice must contain a description of: (1) the incident in general terms; (2) the type of personal information compromised; (3) the general acts of the business to protect the information from further unauthorized access; (4) a telephone number to call for further information or assistance; (5) advice that directs the person to remain vigilant by monitoring accounts and free credit reports.

Notification Recipients

Any affected MI resident, or owner or licensor if notifier is not the owner of licensor of the personal information. If notifying more than 1,000 MI residents, must notify national consumer reporting agencies, unless entity is a financial institution regulated by GLB.

Attorney General Publishes Breach Data

No.

Private Right of Action Included

No.

Exception to Notification Obligation Exists if the Entity is Complying with Other Laws (HIPPA, GLB, etc.)

Entities in compliance with GLB Act, financial institution regulated for compliance with the interagency guidance or HIPAA Privacy Rule.

Allows Flexibility in Notification Requirements to Entities that Maintain Their Own Notification Procedures Consistent with the Statute

No.

Additional Exceptions

Public utility that sends monthly billing or account statements to customers’ postal address may alternatively provide notice by providing all of the following: (1) Electronic notice, if any of the following conditions are met: (a) recipient has expressly consented to receive electronic notice; (b) person or agency has an existing business relationship with the recipient that includes periodic e-mail communications and based on those communications the person or agency reasonably believes that it has the recipient’s current e-mail address; or (c) the person or agency conducts its business primarily through internet account transactions or on the internet; (2) Notification to media reasonably calculated to inform customers of breach; (3) Conspicuous posting of notice on website; and (4) Written notice sent in conjunction with monthly billing or account statement to customer at customer’s postal address.

Penalties for Violations

Attorney general or prosecutor may bring an action to recover fines NTE \$250 for each failure to provide notice, with a maximum aggregate liability for fines arising from the same security breach of \$750K.



Minnesota

Minn. Stat §§ 325E.61, 325E.64, 8.31

Definition of Breach

Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. As applicable to government entities: unauthorized acquisition of data maintained by a government entity that compromises the security and classification of the data.

Definition of Personally Identifiable Information

As applicable to non-government entities: an individual’s first name or first initial and last name in combination with any one or more of the following data elements: (1) SSN; (2) driver’s license number or MN ID card number; (3) 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.

As applicable to government entities: all private or confidential data on individuals in which any individual is or can be identified as the subject of that data, unless the appearance of the name or other identifying data can be clearly demonstrated to be only incidental to the data and the data are not accessed by the name or other identifying data of any individual.

Form of Data

Computerized.

Paper Records Covered

No.

Encrypted Data Covered When the Encryption Key Has Been Accessed or Acquired

No.

Entities Covered

Any person or business that conducts business in MN, and that owns or licenses or maintains personal information. Also, any government entity that collects, creates, receives, maintains, or disseminates private or confidential data on individuals.

Notification Obligation Triggers After Discovery or After Reasonable Investigation

Discovery or notification of the breach.

Time for Notification Once an Obligation is Triggered

As applicable to non-government entities: If notifying MN resident, in the most expedient of time and without unreasonable delay. “Immediately,” if notifying data owner or licensee. If notifying more than 500 MN residents, must notify national consumer reporting agencies of timing, distribution and content of notices within 48 hours of discovery of circumstances requiring notification.

As applicable to government entities: In the most expedient time possible and without unreasonable delay. If notifying more than 1,000 MN residents, must notify national consumer reporting agencies of timing, distribution, and content of notices without unreasonable delay.

Risk of Harm Trigger for Notification Exists

No.

Notification Method

(1) Written notice; (2) Electronic notice, if person’s primary method of communication with individual is by electronic means, or if notice provided is consistent with provisions re electronic records and signatures in 15 U.S.C.; or (3) Substitute notice if person or business demonstrates that the cost of notice will exceed \$250K, the affected class exceeds 500,000, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following: (A) e-mail if person or business has an e-mail address for affected individual, (B) conspicuous posting of notice on Web site page of person or business, if person or business maintains one; and (C) notification to major statewide media.

Mandatory Notification Items

No applicable provision.

Notification Recipients

As applicable to non-government entities: any affected MN resident, or owner or licensee if the notifier is not the owner or licensee of the personal information. If required to notify more than 500 MN residents at a single time, must also notify national consumer reporting agencies as defined in 15 U.S.C. 1681a of the timing, and content of the notices within 48 hours.

As applicable to government entities: any affected individual. If required to notify more than 1,000 individuals at a single time, must also notify national consumer reporting agencies as defined in 15 U.S.C. 1681a of the timing, and content of the notices without unreasonable delay.

Attorney General Publishes Breach Data

No.

Private Right of Action Included

Yes.

Exception to Notification Obligation Exists if the Entity is Complying with Other Laws (HIPPA, GLB, etc.)

Financial institutions as defined by 15 USC 6809(3). No applicable provision for government entities.

Allows Flexibility in Notification Requirements to Entities that Maintain Their Own Notification Procedures Consistent with the Statute

Yes, however no applicable provision for government entities.

Penalties for Violations

As applicable to non-government entities: AG and any individual injured by a violation of this section may enforce under section 8.31. As applicable to government entities: any individual injured by a violation of this chapter may bring action for damages plus costs and reasonable attorney fees.

Miscellaneous Provisions

Forbids businesses accepting payment cards from storing the card security code data, the PIN verification code number, or the full contents of any track of magnetic stripe data after the transaction is authorized. In the event of a breach, entities violating this section are liable for reimbursing the financial institution issuing the, payment cards for any costs and damages suffered by the financial institution as a result of the breach (e.g., fraudulent charges, costs of replacing cards).

Government entities must conduct comprehensive security assessments of any personal information it maintains at least once a year. Personal information is defined as it applies to non-government entities under Minn. Stat. § 325E.61(1)(e).



Mississippi

Miss. Code § 75-24-29

Definition of Breach

Unauthorized acquisition of electronic files, media, databases or computerized data containing personal information of any resident of this state.

Definition of Personally Identifiable Information

An individual’s first name or first initial and last name in combination with any one or more of the following data elements: (1) Social security number; (2) DL number or state ID card number; (3) 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.

Form of Data

Electronic files, media, databases or computerized data.

Paper Records Covered

No.

Encrypted Data Covered When the Encryption Key Has Been Accessed or Acquired

No.

Entities Covered

Any person who conducts business in MS and, who in the course of business, owns, licenses, or maintains personal information of any MS resident.

Notification Obligation Triggers After Discovery or After Reasonable Investigation

After discovery or notification of security breach, following completion of investigation to determine nature and scope of incident, to identify affected individuals or to restore the reasonable integrity of data system. Notification not required if person determines that breach will not likely result in harm to affected individuals. If not data owner, must notify as soon as practicable following discovery, if personal information was, or is reasonably believed to have been, acquired by an unauthorized person for fraudulent purposes.

Time for Notification Once an Obligation is Triggered

“Without unreasonable delay” if data owner or licensee; “as soon as practicable,” if only maintaining data.

Risk of Harm Trigger for Notification Exists

Yes, but not only maintaining data.

Notification Method

(1) Written notice, (2) Telephone notice, (3) Electronic notice, if person’s primary means of communication with affected individuals is by electronic means or if notice is consistent the provisions regarding electronic records and signatures in 15 U.S.C. § 7001; or (4) Substitute notice, if person demonstrates that providing notice would exceed \$5K, affected class of consumers exceeds 5,000, or person does not have sufficient contact information. Substitute notice shall consist of all of the following: (A) e-mail, if e-mail address has been obtained; (B) conspicuous posting of notice of Web site of person if one is maintained; and (C) notification to major statewide media, including newspapers, radio and television.

Mandatory Notification Items

No applicable provision.

Notification Recipients

Affected MS resident, or owner or licensee if the notifier is not the owner or licensee of the personal information.

Attorney General Publishes Breach Data

No.

Private Right of Action Included

No.

Exception to Notification Obligation Exists if the Entity is Complying with Other Laws (HIPPA, GLB, etc.)

Yes, an entity that maintains security breach procedure pursuant to rules, regs, procedures or guidelines established by the primary or federal functional regulator shall be deemed compliant with security breach notifications of this section.

Allows Flexibility in Notification Requirements to Entities that Maintain Their Own Notification Procedures Consistent with the Statute

Yes.

Penalties for Violations

Failure to comply with requirements constitutes an unfair trade practice and shall be enforced by AG.



Missouri

Mo. Rev. Stat. § 407.1500

Definition of Breach

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.

Definition of Personally Identifiable Information

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) SSN; (b) DL 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.

Form of Data

Computerized.

Paper Records Covered

No.

Encrypted Data Covered When the Encryption Key Has Been Accessed or Acquired

No.

Entities Covered

Any person that: (i) owns, licenses, or maintains personal information of a MO resident or (ii) conducts business in MO that owns, licenses or maintains personal information in any form of a MO resident.

Notification Obligation Triggers After Discovery or After Reasonable Investigation

Notification or discovery of security breach, but notification not required if, after an appropriate investigation by the person or after consultation with the relevant federal, state, or local law enforcement agencies, 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.

Time for Notification Once an Obligation is Triggered

“Without unreasonable delay” or “immediately,” if notifying data owner or licensee.

Risk of Harm Trigger for Notification Exists

Yes.

Notification Method

(1) Written notice; (2) Electronic notice for those consumers for whom the person has a valid e-mail address and who have agreed to receive communications electronically, if the notice provided is consistent with the provisions of 15 U.S.C. Section 7001 regarding electronic records and signatures for notices legally required to be in writing; (3) Telephonic notice, if such contact is made directly with the affected consumers; or (4) Substitute notice, if the person demonstrates that the cost of providing notice would exceed \$100K, the class of affected consumers to be notified exceeds 150,000 or the person does not have sufficient contact information or consent, for only those affected consumers without sufficient contact information or consent or the person is unable to identify particular affected consumers, for only those unidentifiable consumers. Substitute notice shall consist of all the following: (a) E-mail notice when the person has an e-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.

Mandatory Notification Items

At a minimum, shall include a description of the following: (a) The incident in general terms; (b) 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.

Notification Recipients

Any affected MO resident, or owner or licensee if notifier is not the owner or licensee of the data. If person must notify more than 1,000 consumers, must notify, without unreasonable delay, the AG and all national consumer reporting agencies of timing, distribution and content of the notice.

Attorney General Publishes Breach Data

No.

Private Right of Action Included

No.

Exception to Notification Obligation Exists if the Entity is Complying with Other Laws (HIPPA, GLB, etc.)

Yes, (1) person that complies with federal/state security breach notification requirements established by its primary or functional state or federal regulator is deemed to be in compliance with this section; (2) financial institution subject to and in compliance with (a) the Federal Interagency Guidance Response Programs for Unauthorized Access to Customer Info and Customer Notice; (b) the National Credit Union Admin regulations in 12 C.F.R. Part 748; or (c) Title V of the GLB Act shall be deemed to be in compliance with this section.

Allows Flexibility in Notification Requirements to Entities that Maintain Their Own Notification Procedures Consistent with the Statute

Yes.

Penalties for Violations

AG has exclusive authority to bring an action for a “willful and knowing” violation of this section and may seek a civil penalty NTE \$150K per breach of the security system or series of breaches of a similar nature that are discovered in a single investigation.

Miscellaneous Provisions

Notification not required if covered entity determines that a risk of identity theft or other fraud to any consumer is not reasonably likely to occur as a result of the breach. However, determination must be documented in writing and maintained for five years.



Montana

Mont. Code Ann. §§ 30-14-1701 - 1705

Definition of Breach

Unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information...and causes or is reasonably believed to cause loss or injury to a person.

Definition of Personally Identifiable Information

Individual’s first name or first initial and last name, in combination with one or more additional elements, when either the name or the data elements are not encrypted: (a) SSN; (b) DL number, state ID card number or tribal ID 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; (e) taxpayer identification number; or (f) an identity protection personal identification number issued by the IRS.

Form of Data

Computerized.

Paper Records Covered

No.

Encrypted Data Covered When the Encryption Key Has Been Accessed or Acquired

No.

Entities Covered

Any person or business that conducts business in MT and that owns, licenses, or maintains computerized data that includes personal information.

Notification Obligation Triggers After Discovery or After Reasonable Investigation

Notification or discovery of security breach.

Time for Notification Once an Obligation is Triggered

“Without unreasonable delay” or “immediately,” if not data owner.

Risk of Harm Trigger for Notification Exists

Yes, definition of “breach of the security of the data system,” includes a determination that the unauthorized acquisition of computerized data “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.”

Notification Method

(1) Written notice; (2) Electronic notice, if notice provided is consistent with the provisions regarding electronic records and signatures in 15 U.S.C. § 7001; (3) Telephonic notice; or (4) Substitute notice, if person or business demonstrates that the cost of providing notice would exceed \$250K, affected class of consumers exceeds 500,000, person or business does not have sufficient contact information. Substitute notice shall consist of the following: (A) e-mail, if e-mail address has been obtained; (B) conspicuous posting of the notice on the website page, if one is maintained; and (C) notification to major statewide media.

Mandatory Notification Items

If notice suggests that the resident may obtain a copy of his file from a consumer reporting agency, business must coordinate with consumer reporting agency as to timing, content, and distribution of notice.

Notification Recipients

Affected MT resident, or owner or licensee of the information if notifier is not the owner or licensee of the information. Must simultaneously submit an electronic copy of notification and statement providing date and method of distribution of notification to the AG’s consumer protection office. All licensees or insurance-support organizations must submit a copy of any required notification and a statement providing the date and method of distribution of the notification to the insurance commissioner.

Attorney General Publishes Breach Data

Yes.

Private Right of Action Included

No.

Exception to Notification Obligation Exists if the Entity is Complying with Other Laws (HIPPA, GLB, etc.)

No.

Allows Flexibility in Notification Requirements to Entities that Maintain Their Own Notification Procedures Consistent with the Statute

Yes.

Penalties for Violations

AG may bring action pursuant to Mont. Code § 30-14-111, and covered entity may be liable for civil penalties NTE \$10k per violation, plus additional civil penalties NTE \$10k per willful violation under Mont. Code § 30-14-142.





Nebraska

Neb. Rev. Stat. §§ 87-801 to 807

Definition of Breach

Unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an individual or commercial entity.

Definition of Personally Identifiable Information

(a) An individual’s first name or first initial and last name in combination with any one or more of the following data elements: (1) SSN; (2) driver’s license number or state ID card 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) unique biometric data; (5) unique electronic ID number or routing code, in combination with any required security code, access code, or password; or (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.

Form of Data

Computerized.

Paper Records Covered

No.

Encrypted Data Covered When the Encryption Key Has Been Accessed or Acquired

Yes, if the confidential process or key was or is reasonably believed to have been acquired as a result of the breach.

Entities Covered

An individual or a commercial entity that conducts business in NE and owns, licenses, or maintains computerized personal information of a NE resident.

Notification Obligation Triggers After Discovery or After Reasonable Investigation

When an individual or a commercial entity “becomes aware” of a breach, and conducts an investigation as to whether harm is likely, and determines that the use of information about a NE resident for an unauthorized purpose has occurred or is reasonably likely to occur.

Time for Notification Once an Obligation is Triggered

“As soon as possible” and “without unreasonable delay” and notice shall be given when entity “becomes aware,” if notifying data owner.

Risk of Harm Trigger for Notification Exists

Yes.

Notification Method

(1) Written notice; (2) Telephonic notice; (3) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. 7001, as such section existed on January 1, 2006; or (4) Substitute notice, if the individual or commercial entity required to provide notice 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 under this subdivision requires all of the following: (A) E-mail notice, if individual or commercial entity has e-mail addresses for the members of the affected class of NE residents; (B) Conspicuous posting of notice on web site of individual or commercial entity if the individual or commercial entity maintains a web site; and (C) Notice to major statewide media outlets. Further substitute notice shall be given to individual or entity that has 10 or fewer employees and demonstrates the cost of providing notice will exceed \$10K, in such case notice shall be given by (i) e-mail if individual or commercial entity has e-mail addresses of affected individuals; (ii) notification by paid advertisement in a local newspaper; (iii) conspicuous posting of the notice on the web site of individual or commercial entity if web site is maintained; and (iv) notification to major media outlets in geographic area where individual or commercial entity is located.

Mandatory Notification Items

No applicable provision.

Notification Recipients

Affected resident in NE, or owner or licensee of the information if notifier is not the owner or licensee of information. Must also notify AG. Notice to AG must not be later than notice to residents.

Attorney General Publishes Breach Data

No.

Private Right of Action Included

No.

Exception to Notification Obligation Exists if the Entity is Complying with Other Laws (HIPPA, GLB, etc.)

Yes, entities regulated by federal or state law that notify in accordance with those federal or state laws are exempt.

Allows Flexibility in Notification Requirements to Entities that Maintain Their Own Notification Procedures Consistent with the Statute

Yes.

Additional Exceptions

Information provided pursuant to a court order, search warrant, subpoena or state agency order is not a breach.

Penalties for Violations

AG may issue subpoenas and seek and recover direct economic damages for each affected NE resident injured by a violation of the act.



Nevada

Nev. Rev. Stat. §§ 603A.010 et seq.
Nev. Rev. Stat. §§ 603A.210 et seq.

Definition of Breach

Unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information maintained by the data collector.

Definition of Personally Identifiable Information

An individual’s first name or first initial and last name in combination with any one or more of the following data elements, when the name and data elements are not encrypted: (1) SSN; (2) DL number, driver authorization card number, or ID card 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) A medical identification number or a health insurance identification number; or (5) 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. Does not include last 4 digits of a SSN, DL number. driver authorization card number, or ID card number.

Form of Data

Computerized.

Paper Records Covered

No.

Encrypted Data Covered When the Encryption Key Has Been Accessed or Acquired

No.

Entities Covered

Any data collector that owns, maintains, or licenses computerized data that includes personal information. “Data collector” means any governmental agency, institution of higher education, corporation, financial institution or retail operator or any other type of business entity or association that, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates or otherwise deals with nonpublic personal information.

Notification Obligation Triggers After Discovery or After Reasonable Investigation

Discovery or notification of the security breach.

Time for Notification Once an Obligation is Triggered

“In the most expedient time possible and without unreasonable delay.” “Immediately,” if notifying data owner or licensee.

Risk of Harm Trigger for Notification Exists

Yes, “breach of the security of the system data” is defined as the unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information maintained by the data collector.

Notification Method

(1) Written notification; (2) Electronic notification, if the notification provided is consistent with the provisions 15 U.S.C. §§ 7001 et seq.; (3) Substitute notification, if data collector demonstrates that the cost of providing notification would exceed \$250K, 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: (i) Notification by electronic mail when the data collector has electronic mail addresses for the subject persons; (ii) Conspicuous posting of the notification on the Internet website of the data collector, if the data collector maintains an Internet website; (iii) Notification to major statewide media.

Mandatory Notification Items

No applicable provision.

Notification Recipients

Any affected NV resident, or owner or licensee of personal information if only maintaining personal information. If notifying more than 1,000 persons at one time, data collector must also notify, without unreasonable delay, national consumer reporting agencies (of timing and content of notification).

Attorney General Publishes Breach Data

No.

Private Right of Action Included

Data collector that provides requisite notice may bring suit for damages against a person that unlawfully obtained or benefited from personal information obtained from records maintained by the data collector.

Exception to Notification Obligation Exists if the Entity is Complying with Other Laws (HIPPA, GLB, etc.)

Yes, entities subject to and in compliance with GLB Act are exempt.

Allows Flexibility in Notification Requirements to Entities that Maintain Their Own Notification Procedures Consistent with the Statute

Yes.

Penalties for Violations

AG may bring action to obtain temporary or permanent injunction.

Miscellaneous Provisions

Court may order breach exploiters to pay restitution to costs incurred by data collector in providing notification.

New Hampshire

N.H. Rev. Stat. §§ 359-C:19, C:20, C:21;
358-A:4; 332-I:1–I:610

N.H. Rev. Stat. Ann. § 189:65, 189:66

Definition of Breach

Unauthorized acquisition of computerized data that materially compromises the security or confidentiality of personal information maintained by a person doing business in this state.

Definition of Personally Identifiable Information

An individual’s first name or first initial and last name in combination with any one or more of the following data elements: (1) SSN; (2) DL number or gov’t ID card 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.

Form of Data

Computerized.

Paper Records Covered

No.

Encrypted Data Covered When the Encryption Key Has Been Accessed or Acquired

Yes, if data is acquired in combination with any required key, security code, access code or password that would permit access to the encrypted data.

Entities Covered

Any person in NH doing business that owns, maintains, or licenses computerized data that includes personal information.

Notification Obligation Triggers After Discovery or After Reasonable Investigation

“Becomes aware,” must “promptly” determine likelihood that information has been or will be misused. If 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.

Time for Notification Once an Obligation is Triggered

“As soon as possible” and “immediately,” if notifying data owner.

Risk of Harm Trigger for Notification Exists

Yes.

Notification Method

(1) Written notice; (2) Telephonic notice; (3) Electronic notice, if the agency or business’ primary means of communication with affected individuals is by electronic means; (4) Substitute notice, if 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. Substitute notice shall consist of all of the following: (A) e-mail if e-mail address is obtained; (B) conspicuous posting of notice on person’s business website, if person maintains one; and (C) notification to major statewide media; or (5) Notice pursuant to the person’s internal notification procedures.

Mandatory Notification Items

Notice shall include, at a minimum: (a) description of the incident in general terms; (b) approximate date of breach; (c) type of personal information obtained as a result of the security breach; (d) telephonic contact information of the person subject to this section.

Notice to a regulator or to the AG must include the anticipated date of the notice to the individuals and approximate number of individuals in NH who will be notified.

Notification Recipients

Any affected individual, plus national consumer credit reporting agencies if more than 1,000 people are affected, unless person is subject to GLB Act. Must also notify AG or, if entity is subject to N.H. Rev. Stat. § 358-A:3(l), must also notify the regulator which has primary regulatory authority over it. All entities engaged in trade or commerce must notify the regulator which has primary regulatory authority over such trade or commerce.

Attorney General Publishes Breach Data

Yes: <http://doj.nh.gov/consumer/security-breaches/>.

Private Right of Action Included

Yes.

Exception to Notification Obligation Exists if the Entity is Complying with Other Laws (HIPPA, GLB, etc.)

Yes, entities subject to N.H. Rev. Stat. § 358-A:3(l) who maintain procedures for security breach notification in accordance with state and federal regulations.

Allows Flexibility in Notification Requirements to Entities that Maintain Their Own Notification Procedures Consistent with the Statute

Yes.

Penalties for Violations

Any person injured by violation may bring an action for damages and/or an injunction. AG may also bring action.



New Jersey

N.J. Stat. Ann §§ 56:8-161 - 166

Definition of Breach

Unauthorized access to electronic files, media or data containing personal information that compromises the security, confidentiality or integrity of personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable.

Definition of Personally Identifiable Information

An individual’s first name or first initial and last name in combination with any one or more of the following data elements: (1) SSN; (2) driver’s license number or state ID card 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. Dissociated data that, if linked, would constitute personal information if the means to link the dissociated data were accessed in connection with access to dissociated data.

Form of Data

Electronic files, media, or data.

Paper Records Covered

No.

Encrypted Data Covered When the Encryption Key Has Been Accessed or Acquired

No.

Entities Covered

Any business that conducts business in NJ, or any public entity that compiles or maintains computerized records that include personal information.

Notification Obligation Triggers After Discovery or After Reasonable Investigation

Upon discovery or notification of breach.

Time for Notification Once an Obligation is Triggered

If compiling or maintaining computerized records, “in the most expedient time possible and without unreasonable delay.” If compiling or maintaining computerized records on behalf of another business or public entity, must notify “immediately.”

Risk of Harm Trigger for Notification Exists

Yes, disclosure not required if company determines that misuse of information is not reasonably possible; must document determination and retain for 5 years.

Notification Method

(1) Written notice; (2) Electronic notice, if notice is provided in accordance with 15 U.S.C. §7001; (3) Substitute notice if business or public entity demonstrates that cost of providing notice would exceed \$250K, affected class exceeds 500,000, or the business or public entity does not have sufficient contact information. Substitute notice shall consist of (A) e-mail if person has an e-mail address of the affected person, (B) conspicuous posting of the notice on the Internet web site page of business or public entity, if one is maintained, and (C) notification to major Statewide media.

Mandatory Notification Items

No applicable provision.

Notification Recipients

Affected NJ residents, or business or public entity if notifier maintains information on behalf of business or entity. Must notify state police prior to notifying individuals. If more than 1,000 NJ residents notified at once, must also notify national consumer reporting agencies of timing, distribution and content of notices.

Attorney General Publishes Breach Data

No.

Private Right of Action Included

No.

Exception to Notification Obligation Exists if the Entity is Complying with Other Laws (HIPPA, GLB, etc.)

No.

Allows Flexibility in Notification Requirements to Entities that Maintain Their Own Notification Procedures Consistent with the Statute

Yes.

Penalties for Violations

No penalties provided, however violation constitutes an unlawful practice.



New Mexico

N. M. Stat. Ann. § 57-12C-1 et seq.
2017 H.B. 15, Chap. 36

Definition of Breach

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.

Definition of Personally Identifiable Information

(1) 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.

Form of Data

Computerized data.

Paper Records Covered

No.

Encrypted Data Covered When the Encryption Key Has Been Accessed or Acquired

Yes, if the confidential process or key used to decrypt the encrypted data is also breached.

Entities Covered

Any person that owns or licenses elements that include personal identifying information of a NM resident, or anyone that is licensed to maintain or possess computerized data containing personal identifying information of a NM resident who does not own or license the data.

Notification Obligation Triggers After Discovery or After Reasonable Investigation

When personal identifying information is reasonably believed to have been subject to a security breach.

Time for Notification Once an Obligation is Triggered

In the most expedient time possible, but no later than 45 days following discovery of breach.

Risk of Harm Trigger for Notification Exists

Notification is not required if, after an appropriate investigation, the data owner/licensee determines that the security breach does not give rise to a significant risk of identity theft or fraud.

Notification Method

(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 the requirements of 15 U.S.C. Section 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.

Mandatory Notification Items

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 required to provide notification 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.

(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 Fair Credit Reporting and Identity Security Act.

Notification Recipients

Any NM resident affected by breach, or the data owner. f more than 1000 NM residents are affected, must notify AG and major consumer reporting agencies, and provide the number of NM residents to be notified, as well as a copy of the notification sent to NM residents.

Attorney General Publishes Breach Data

No.

Private Right of Action Included

No.

Exception to Notification Obligation Exists if the Entity is Complying with Other Laws (HIPPA, GLB, etc.)

Exemptions for anyone covered by and in compliance with the GLB Act or HIPAA.

Allows Flexibility in Notification Requirements to Entities that Maintain Their Own Notification Procedures Consistent with the Statute

Anyone that maintains its own notice procedures as part of an information security policy for the treatment of personal identifying information, and whose procedures are otherwise consistent with the timing requirements of this section, is deemed to be in compliance with the notice requirements of this section if the person notifies affected consumers in accordance with its policies in the event of a security breach.

Additional Exceptions

Data breach notification requirements do not apply to the state of NM or any of its political subdivisions.

Penalties for Violations

If the AG brings action for a violation of the Data Breach Notification Act, 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 the Data Breach Notification Act knowingly or recklessly, the court may impose a civil penalty of the greater of \$25,000 or, in the case of failed notification, \$10 per instance of failed notification up to a maximum of \$150,000.

Miscellaneous Provisions

Anyone that owns or licenses personal identifying information of a NM resident must (1) arrange for proper disposal of records when they are no longer needed, such as by shredding, erasing, or otherwise modifying the personal identifying information contained in the records to make the information unreadable or undecipherable.

Anyone that owns or licenses personal identifying information of a NM resident must implement and maintain reasonable security procedures to protect personal identifying information.

Anyone that discloses personal identifying information of a NM resident pursuant to a contract with a service provider must require by contract that the service provider implement and maintain reasonable security procedures and practices.

New York

N.Y. Gen. Bus. Law § 899-aa

Definition of Breach

Unauthorized acquisition or acquisition without valid authorization of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a business.

Definition of Personally Identifiable Information

Personal information is defined as any information concerning a natural person which can be used to identify the person. Private information is personal information in combination with any one or more of the following data elements: (1) SSN; (2) driver’s license number or non-driver ID card number; or (3) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to the individual’s financial account.

Form of Data

Computerized.

Paper Records Covered

No.

Encrypted Data Covered When the Encryption Key Has Been Accessed or Acquired

No.

Entities Covered

Any person or business which conducts business in NY and either owns, licenses, or maintains computerized data that includes private information.

Any state entity that owns or licenses computerized data that includes private information.

Notification Obligation Triggers After Discovery or After Reasonable Investigation

Upon discovery or notification of security breach.

Time for Notification Once an Obligation is Triggered

If data owner or licensee, notification shall be made in the most expedient time possible and without unreasonable delay. If notifying data owner, notice shall be made “immediately.” If reporting entity is subject to regulation by the Department of Financial Services (DFS), must report breach or any material cybersecurity event to the DFS within 72 hours of determining an event has occurred.

Risk of Harm Trigger for Notification Exists

Yes, to determine whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization, business may consider the following factors: (1) indication that info. is in phys. possession and control of an unauthorized person, (2) indication that info. has been downloaded/ copied; or (3) indication that info. was used by an unauthorized person.

Notification Method

(1) Written notice, (2) Electronic notice, if recipient has expressly consented to receiving electronic notice and log is kept, and provided that any person or business shall not require a person to consent to accepting electronic notice as a condition of establishing any business relationship or engaging in any transaction; (3)Telephonic notice if log is kept; or (4)Substitute notice, if business demonstrates to state AG that cost of providing notice would exceed \$250K, or that affected class of subject persons to be notified exceeds 500,000 or such business does not have sufficient contact information. Substitute notice shall consist of (A) e-mail if e-mail address is obtained; (B) conspicuous posting of the notice on the web site page if web site is obtained; and (C) notification to major statewide media.

Mandatory Notification Items

Notice must include contact information for business making the notification, a description of the information that was compromised, including specifically which data elements were compromised.

Notification Recipients

Affected NY residents, plus the AG, the NY State Police, and the NY Dept. of State (notice must include the timing, content and distribution of notices, and approx. number of affected persons). Notification to AG, Police, and Dept. of State may use reporting forms provided here. Non-governmental entities may use online portal to notify AG. If more than 5,000 New York residents are to be notified, consumer reporting agencies must also be notified as to the timing, content and distribution of notices and approx. number of affected persons. If reporting entity is subject to regulation by the Department of Financial Services (DFS), must report breach or any material cybersecurity event to the DFS within 72 hours of determining an event has occurred.

Attorney General Publishes Breach Data

No.

Private Right of Action Included

No, but the state AG may sue on behalf of citizens and obtain damages for them, including consequential financial loss for failure to notify (in addition to imposing civil fines).

Exception to Notification Obligation Exists if the Entity is Complying with Other Laws (HIPPA, GLB, etc.)

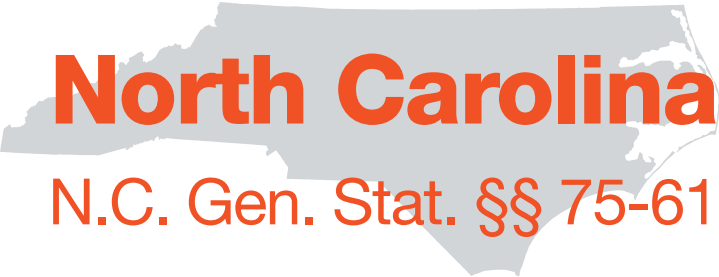
No.

Allows Flexibility in Notification Requirements to Entities that Maintain Their Own Notification Procedures Consistent with the Statute

No.

Penalties for Violations

AG may bring action for injunctive relief; damages, and, if covered entity acted knowingly or recklessly, civil penalties of the greater of \$5K or \$10 per instance of failed notification, NTE \$150K. Action must be brought within two years after violation or discovery of violation.



North Carolina

N.C. Gen. Stat. §§ 75-61, 75-65

Definition of Breach

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.

Definition of Personally Identifiable Information

An individual's first name or first initial and last name in combination with any of the following: (1) SSN or employer taxpayer ID number; (2) DL, state ID, or passport number; (3) checking account number; (4) savings account number; (5) credit card number; (6) debit card number; (7) PIN; (8) digital signature. N.C. Gen. Stat. § 75-61(10). Personal information shall not include electronic ID numbers, electronic mail names or addresses, Internet account numbers, Internet ID names, parent's legal surname prior to marriage, or a password unless this information would permit access to a person's financial account or resources.

Form of Data

Computerized, paper, or otherwise.

Paper Records Covered

Yes.

Encrypted Data Covered When the Encryption Key Has Been Accessed or Acquired

Yes, if the encryption key or confidential process has also been breached.

Entities Covered

Any business that owns or licenses personal information of residents of NC or any business that conducts business in NC that owns or licenses personal information.

Notification Obligation Triggers After Discovery or After Reasonable Investigation

Shall provide notice to affected person that there has been a security breach following "discovery or notification" of the breach which requires "illegal use of the personal information" to have occurred or is "reasonably likely to occur" or that creates "a material risk of harm to a consumer."

Time for Notification Once an Obligation is Triggered

If data owner or licensee, "without legitimate delay." If business maintains data, must notify "immediately."

Risk of Harm Trigger for Notification Exists

Yes.

Notification Method

(1) Written notice; (2) Electronic notice, for those persons for whom it has a valid e-mail address and who have agreed to receive communications electronically if the notice is provided in accordance with 15 U.S.C. § 7001; (3) Telephonic notice, provided that contact is made directly with the affected persons; or (4) Substitute notice, if business demonstrates that the cost of providing notice would exceed \$250,000 or that the affected class of subject persons to be notified exceeds 500,000, or if the business does not have sufficient contact information, 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.

Mandatory Notification Items

Must be "clear and conspicuous" and must contain a description of: (1) the incident in general terms; (2) the type of personal information compromised; (3) the general acts of the business to protect the information from further unauthorized access; (4) a telephone number to call for further information or assistance, if one exists; (5) advice that directs the person to remain vigilant by monitoring accounts and free credit reports; (6) toll-free numbers and addresses for the major consumer reporting agencies; (7) toll-free numbers, addresses and web site addresses for the FTC and the NC AG's office, along with a statement that the individual can obtain information from these sources about preventing identity theft.

Notification Recipients

All persons affected, not just NC residents. If a business provides notice to an affected person, the business shall notify, without unreasonable delay, the Consumer Protection Division of the AG's office as well as all nationwide consumer reporting agencies. Such notice shall describe the nature of the breach, steps taken to prevent a similar breach in the future and information regarding the timing, distribution and content of the notice.

If a business provides notice to more than 1000 persons at one time, business shall notify, without unreasonable delay, the Consumer Protection Division of the AG's Office and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution and content of the notice.

Attorney General Publishes Breach Data

No.

Private Right of Action Included

Yes, only if an individual is injured as a result of a violation of this section.

Exception to Notification Obligation Exists if the Entity is Complying with Other Laws (HIPPA, GLB, etc.)

Yes, financial institutions that are subject to and in compliance with the Federal Interagency Guidance are deemed to be in compliance with this section.

Allows Flexibility in Notification Requirements to Entities that Maintain Their Own Notification Procedures Consistent with the Statute

No.

Penalties for Violations

A violation of this section is a violation of N.C. Gen. Stat § 75-1.1 (Unfair and deceptive act).

North Dakota

N.D. Cent. Code §§ 51-30-01 et seq.;
51-15-11; 51-15-07

Definition of Breach

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.

Definition of Personally Identifiable Information

An individual’s first name or first initial and last name in combination with any of the following data elements, when the name and the data elements are not encrypted: (1) The individual’s social security number; (2) The operator’s license number assigned to an individual by the department of transportation under section 39-06-14; (3) A nondriver color photo identification card number assigned to the individual by the department of transportation under section 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.

Form of Data

Computerized.

Paper Records Covered

No.

Encrypted Data Covered When the Encryption Key Has Been Accessed or Acquired

No.

Entities Covered

Any person that conducts business in ND that owns, licenses, or maintains computerized personal information.

Notification Obligation Triggers After Discovery or After Reasonable Investigation

Notification or discovery of the breach.

Time for Notification Once an Obligation is Triggered

If person owns or licenses personal information, notification must be made “in the most expedient time possible and without unreasonable delay.” If person maintains personal information, notification must be made “immediately” following the discovery of the breach.

Risk of Harm Trigger for Notification Exists

No.

Notification Method

(1) Written notice; (2) Electronic notice, if the notice provided is in accordance with 15 U.S.C. § 7001; or (3) Substitute notice, if the person 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 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.

Mandatory Notification Items

No applicable provision.

Notification Recipients

Any affected ND resident, or the owner or licensee of the information if the notifier is not the owner or licensee of the information. If breach affects 250 or more N.D. residents, must notify ND AG.

Attorney General Publishes Breach Data

No.

Private Right of Action Included

No.

Exception to Notification Obligation Exists if the Entity is Complying with Other Laws (HIPPA, GLB, etc.)

Yes, financial institutions that comply with notification requirements under Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice are deemed to be in compliance.

Allows Flexibility in Notification Requirements to Entities that Maintain Their Own Notification Procedures Consistent with the Statute

Yes.

Penalties for Violations

AG may bring action.



Definition of Breach

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.

Definition of Personally Identifiable Information

An individual’s first name or first initial and last name in combination with any one or more of the following data elements: (1) SSN; (2) DL number or state ID card 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.

Form of Data

Computerized.

Paper Records Covered

No.

Encrypted Data Covered When the Encryption Key Has Been Accessed or Acquired

No.

Entities Covered

Individual or business entity conducting business in OH that owns, licenses, is custodian of or stores computerized data that includes personal information.

Notification Obligation Triggers After Discovery or After Reasonable Investigation

After discovery or notification of the breach, if access and acquisition by unauthorized person causes or reasonably is believed will cause a material risk of identity theft or other fraud to the resident.

Time for Notification Once an Obligation is Triggered

If person owns or licenses the personal information, in the most expedient time possible, but not later than 45 days.

If person is custodian of or stores computerized data, shall notify that other person or governmental entity of any breach in “an expeditious manner.”

Risk of Harm Trigger for Notification Exists

Yes.

Notification Method

(1) Written notice, (2) Telephonic notice, (3) E-mail notice if e-mail is the primary means of communication; or (4) Substitute notice permitted if the individual or commercial entity demonstrates that the cost of providing notice will exceed \$250K, affected class of consumers exceeds 500,000, or individual or commercial entity does not have sufficient contact information. Substitute notice shall consist of (A) e-mail if e-mail addresses have been obtained; (B) conspicuous posting of disclosure or notice on web site, if web site is maintained; and (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 75% of the population of OH.

If covered entity is a business with ten or fewer employees and demonstrates that cost of providing notice will exceed \$10K, may provide substitute notice to consist of all of the following: (a) Notification by a paid advertisement (of sufficient size that it covers at least 1/4 of page) in a local newspaper that is distributed in the geographic area in which business is located, to be published at least once a wk for 3 wks; (b) Conspicuous posting of the disclosure or notice on the business website, if it maintains one; and (c) Notification to major media outlets in the geographic area in which business is located.

Mandatory Notification Items

No applicable provision.

Notification Recipients

Any affected resident; or owner, licensee or governmental entity, if person is not owner or licensee. If more than 1,000 OH residents notified, must notify national consumer reporting agencies. All entities with a license or certificate of authority from the superintendent of insurance must notify the Dept of Insurance within 15 days of discovering a loss of control of policyholder’s personal information if over 250 OH residents are affected.

Attorney General Publishes Breach Data

No.

Private Right of Action Included

No.

Exception to Notification Obligation Exists if the Entity is Complying with Other Laws (HIPPA, GLB, etc.)

Yes, (1) Financial institution, trust company, or credit union that is required by federal law, regulation, regulatory guidance, or other regulatory action to notify its consumers, and is subject to regulatory review for compliance, is exempt; (2) Covered entities subject to HIPAA are exempt.

Allows Flexibility in Notification Requirements to Entities that Maintain Their Own Notification Procedures Consistent with the Statute

No.

Additional Exceptions

Acquisition of personal information pursuant to a search warrant, subpoena, or court/regulatory agency order is not a breach.

Penalties for Violations

AG may bring action.

Oklahoma

Okla. Stat.tit. 24 § 161 et seq.

Definition of Breach

Unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes, or the individual or entity reasonably believes has caused or will cause, identity theft or other fraud to any resident of this state.

Definition of Personally Identifiable Information

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 neither encrypted nor redacted: (1) SSN; (2) DL number or state ID number issued in lieu of DL; (3) financial acct. number, or credit 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.

Form of Data

Computerized.

Paper Records Covered

No.

Encrypted Data Covered When the Encryption Key Has Been Accessed or Acquired

Yes, if encrypted information is accessed and acquired in an unencrypted form or if the security breach involves a person with access to the encryption key and the individual or entity reasonably believes that such breach has caused or will cause identity theft or fraud to any OK resident.

Entities Covered

Any individual or entity that owns, licenses, or maintains computerized data that includes personal information of OK resident.

Notification Obligation Triggers After Discovery or After Reasonable Investigation

Discovery or notification of the security breach, if unencrypted and unredacted PI of an OK resident 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.

Time for Notification Once an Obligation is Triggered

“Without unreasonable delay,” and “as soon as practicable” if notifying the data owner.

Risk of Harm Trigger for Notification Exists

Yes, must cause or reasonably believed to have caused or will cause identity theft or other fraud.

Notification Method

(1) Written notice; (2) Telephone notice, (3) Electronic notice; or (4) Substitute notice, if the individual or entity demonstrates that the cost of providing notice will exceed more than \$50K, affected class of consumers exceeds 100,000, or individual or entity does not have sufficient contact information. Substitute notice shall consist of any two 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 Internet web site of the individual or the entity if the individual or the entity maintains a public Internet web site; or (c) notice to major statewide media.

Mandatory Notification Items

No applicable provision.

Notification Recipients

Any affected resident, or owner or licensee if notifier is not the owner or licensee of the personal information.

Attorney General Publishes Breach Data

No.

Private Right of Action Included

No.

Exception to Notification Obligation Exists if the Entity is Complying with Other Laws (HIPPA, GLB, etc.)

Yes, (1) financial institution that complies with notification requirements under Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice; (2) entity that complies with notification requirements or procedures pursuant to the rules, regulation, procedures or guidelines established by the primary or functional federal regulator of the entity.


Allows Flexibility in Notification Requirements to Entities that Maintain Their Own Notification Procedures Consistent with the Statute

Yes.

Penalties for Violations

AG or district attorney may bring an action in same manner as an unlawful practice under the OK Consumer Protection Act. AG or district attorney may obtain either actual damages for a violation of this act or a civil penalty NTE \$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.

Violation by a state-chartered or state-licensed financial institution shall be enforceable exclusively by the primary state regulator of the financial institution.



Oregon

Or. Rev. Stat. §§ 646A.600–.604, 646A.624–.626;
S.B. 1551

Definition of Breach

Unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information that a person maintains.

Definition of Personally Identifiable Information

An individual’s first name or first initial and last name in combination with any one or more of the following data elements: (1) SSN; (2) DL number or state ID card number; (3) passport number or other US-issued ID card number; (4) 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, 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; (5) data from automatic measurements of physical characteristics, such as an image of a fingerprint, retina or iris, that are used to authenticate an individual’s identity in the course of a financial transaction or other transaction; (6) health insurance policy number or health insurance subscriber ID number in combination with any other unique identifier that a health insurer uses to identify an individual; (7) information about medical history or mental or physical condition or about a health care professional’s medical diagnosis or treatment of an individual.

Any of the above elements when not combined with the individual’s first name or first initial and last name if: (1) compromised data is unencrypted, not redacted, or has not been rendered unusable; and (2) compromised data would enable identity theft against subject of data.

Form of Data

Computerized.

Paper Records Covered

No.

Encrypted Data Covered When the Encryption Key Has Been Accessed or Acquired

No.

Entities Covered

Any person that owns, licenses, maintains or otherwise possesses data that includes a consumer’s (i.e., OR resident’s) personal information that is used in the course of the person’s business, vocation, occupation or volunteer activities and was subject to a breach of security.

Notification Obligation Triggers After Discovery or After Reasonable Investigation

Discovery or notification of the breach, except notification not required if, after an appropriate investigation or after consultation with relevant federal, state or local law enforcement agencies, the person determines that no reasonable likelihood of harm to the consumers whose personal information has been acquired has resulted or will result from the breach (determination must be documented in writing and maintained for five years).

Time for Notification Once an Obligation is Triggered

In the most expeditious time possible and without unreasonable delay, but no later than 45 days after discovery of the breach.

Risk of Harm Trigger for Notification Exists

Yes.

Notification Method

(a) Written notice; (b) Electronic notice if person’s customary method of communication with the consumer is by electronic means or is consistent with 15 U.S.C. 7001, as that Act existed on Oct. 1, 2007; (c) Telephone notice, provided that contact is made directly with the affected consumer; or(d) Substitute notice, if the person demonstrates that the cost of providing notice would exceed \$250K, that the affected class of consumers to be notified exceeds 350,000, or if the person does not have sufficient contact information to provide notice. Substitute notice consists of the following: (A) Conspicuous posting of the notice or a link to the notice on the Internet home page of the person if the person maintains one; and (B) Notification to major statewide television and newspaper media.

Mandatory Notification Items

Notice must include: a) description of incident in general terms; b) approximate date of the breach; c) type of personal information obtained as a result of the breach; d) contact information of entity notifying consumer; e) contact information for national consumer reporting agencies; and f) advice to individual to report suspected identity theft to law enforcement, including FTC.

Notification Recipients

Any affected person, or owner or licensor of information if notifier is not the owner or licensor of the information. If breach affects more than 250 Oregon residents, must notify AG and include a copy of the notice provided affected individuals through online portal. If notifying more than 1,000 OR residents, must also notify, “without unreasonable delay,” nationwide consumer reporting agencies as to the timing, distribution and content of notice, and include any police report number assigned to the breach.

Attorney General Publishes Breach Data

Yes: <https://justice.oregon.gov/consumer/databreach/>.

Private Right of Action Included

No.

Exception to Notification Obligation Exists if the Entity is Complying with Other Laws (HIPPA, GLB, etc.)

Yes, (1) Persons complying with notification requirements that provide greater protection to personal info and similar or greater disclosure requirements pursuant to rules promulgated by person’s primary federal regulator; (2) Persons complying with state or federal law providing more protection and similar or greater disclosure requirements than OR law; and (3) Persons subject to and compliant with GLB Act.

Allows Flexibility in Notification Requirements to Entities that Maintain Their Own Notification Procedures Consistent with the Statute

No.

Penalties for Violations

Civil penalty of not more than \$1,000 per violation for a max of \$500,000. Every violation is a separate offense, with each day’s continuance a separate violation.

Miscellaneous Provisions

Requires persons storing personal information to develop, implement, and maintain “reasonable safeguards” to protect the security, confidentiality, and integrity of the personal information, including disposal of data.

Pennsylvania

73 Pa. Cons. Stat. §2301–2308, 2329;
201-4, 201-4.1, 201-8

Definition of Breach

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.

Definition of Personally Identifiable Information

An individual’s first name or first initial and last name in combination with any one or more of the following data elements: (1) SSN; (2) DL number or state ID card 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.

Form of Data

Computerized.

Paper Records Covered

No.

Encrypted Data Covered When the Encryption Key Has Been Accessed or Acquired

Yes, if information is acquired in unencrypted form, if the breach involves the security of the encryption, or if it involves a person with access to the key.

Entities Covered

An entity that maintains, stores, or manages computerized data that includes personal information. A vendor that maintains, stores, or manages computerized data on behalf of another entity.

Notification Obligation Triggers After Discovery or After Reasonable Investigation

Following discovery of breach.

Time for Notification Once an Obligation is Triggered

“Without unreasonable delay” and “following discovery,” if notifying the data owner.

Risk of Harm Trigger for Notification Exists

Yes.

Notification Method

(1) Written notice to individual’s last known home address; (2) Telephonic notice; (3) E-mail notice, if a prior business relationship exists and the person or entity has a valid e-mail address for the individual; or (4) Substitute notice, if the entity demonstrates one of the following: (i) The cost of providing notice would exceed \$100,000. (ii) The affected class of subject persons to be notified exceeds 175,000. (iii) The entity does not have sufficient contact information. 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.

Mandatory Notification Items

If telephonic notice given, must be given in a “clear and conspicuous manner,” describe the incident in general terms, and verify the personal information compromised without requiring the customer to provide personal info. Customer must also be provided with a phone number or website for more informtion or assistance.

Notification Recipients

Any affected resident at their PA address. If giving notice to more than 1,000 PA residents at once, all consumer reporting agencies as to the timing, distribution, and number of notices.

Attorney General Publishes Breach Data

No.

Private Right of Action Included

No.

Exception to Notification Obligation Exists if the Entity is Complying with Other Laws (HIPPA, GLB, etc.)

Yes, (1) A financial institution in compliance with the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, or (2) an entity in compliance with notification requirements or procedures pursuant to rules, regulations, procedures or guidelines established by the entity’s primary or functional Federal regulator are deemed in compliance with this act.

Allows Flexibility in Notification Requirements to Entities that Maintain Their Own Notification Procedures Consistent with the Statute

Yes.

Penalties for Violations

A violation of this Act is an unfair or deceptive trade practice and the state AG is charged with enforcement.



Puerto Rico

10 P.R. Laws Ann. §§ 4051–4055

Definition of Breach

(1) Access is permitted to unauthorized persons or entities to data files such that the security, confidentiality, or integrity of the information in the data bank has been compromised, or (2) it is known or there is a reasonable suspicion that a person or entity that is normally authorized to have access has violated the professional confidentiality or obtained authorization under false representation with the intention of making illegal use of the information.

Definition of Personally Identifiable Information

A file containing at least the name or first initial and the surname of a person, together with any of the following data: (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.

Form of Data

Legible enough so that in order to access it there is no need to use a special cryptographic code.

Paper Records Covered

No.

Encrypted Data Covered When the Encryption Key Has Been Accessed or Acquired

No.

Entities Covered

Any entity that is the owner or custodian of a database that include personal information of citizens residents of Puerto Rico, or any entity that resells or provides access to digital data banks that contain personal information files of citizens.

Notification Obligation Triggers After Discovery or After Reasonable Investigation

Discovery of the breach.

Time for Notification Once an Obligation is Triggered

Must notify clients expeditiously as possible; must notify the Department of Consumer Affairs within 10 days, which must make an announcement to the public within 24 hours after being notified.

Risk of Harm Trigger for Notification Exists

No.

Notification Method

Written direct notice to those affected by mail or by authenticated electronic means according to the Digital Signatures Act. However, if the above method is excessively burdensome due to the number of people affected, the difficulty in locating all the affected people or to the economic situation of the enterprise or entity, or the cost exceeds \$100,000 or more than 100,000 people must be notified, notice may be provided by (1) prominent display of an announcement to that respect at the entity’s 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 (2) a communication to that respect to the media informing of the situation and providing information as to how to contact the entity to allow for better follow-up. When the information is of relevance to a specific professional or commercial sector, the announcement may be made through publications or programming of greater circulation oriented towards that sector.

Mandatory Notification Items

Notice should include a toll free number and a website for people to obtain information or assistance.

Notification Recipients

Any citizen of Puerto Rico affected by the breach, as well as the Department of Consumer Affairs.

Attorney General Publishes Breach Data

No.

Private Right of Action Included

Yes.

Exception to Notification Obligation Exists if the Entity is Complying with Other Laws (HIPPA, GLB, etc.)

No applicable provision.

Allows Flexibility in Notification Requirements to Entities that Maintain Their Own Notification Procedures Consistent with the Statute

Yes..

Penalties for Violations

The Secretary may impose fines of \$500 to \$5000 for each violation.

Miscellaneous Provisions

If the breach occurs in the database of a government agency or public corporation, the Citizen’s Advocate Office must be notified.



Rhode Island

R.I. Gen Laws §§ 11-49.3-2 to 11-49.3-6

Definition of Breach

Unauthorized access or acquisition of unencrypted computerized data information that compromises the security, confidentiality, or integrity of personal information maintained by the municipal state, state agency, or person.

Definition of Personally Identifiable Information

An individual’s first name or first initial and last name in combination with any one or more of the following data elements: (1) SSN; (2) driver’s license number, RI ID card number, or tribal ID number; (3) account number, credit, or debit card number, in combination with any required security code, access code, password, or PIN, that would permit access to an individual’s financial account; (4) medical or health insurance info; (5) e-mail address with any required security code, access code, or password that would permit access to an individual’s personal, medical, insurance, or financial account.

Form of Data

Computerized.

Paper Records Covered

No.

Encrypted Data Covered When the Encryption Key Has Been Accessed or Acquired

No.

Entities Covered

Any municipal agency, state agency, or person that stores, owns, collects, processes, maintains, acquires, uses, or licenses data that includes personal information.

Notification Obligation Triggers After Discovery or After Reasonable Investigation

Confirmation of the breach and the ability to ascertain the information required to fulfill notice requirements.

Time for Notification Once an Obligation is Triggered

Must notify consumers within 45 days of confirmation of breach, in the most expedient time possible.

Risk of Harm Trigger for Notification Exists

Yes.

Notification Method

(1) Written notice; (2) Electronic notice, if the notice is in accordance with 15 U.S.C. § 7001; (3) Substitute notice, if the notifier demonstrates that the cost of providing notice would exceed \$25K, or that the affected class of subject persons to be notified exceeds 50,000, or the notifier does not have sufficient contact information. Substitute notice shall consist of all of the following: (A) E-mail notice when the notifier has an e-mail address for the subject persons; (B) Conspicuous posting of the notice on the notifier’s website page, if the notifier maintains one; (C) Notification to major statewide media.

Mandatory Notification Items

Notification must include, to the extent known: (1) general and brief description of the incident, including how breach occurred and number of affected individuals; (2) type of info that was subject to breach; (3) date of breach, estimated date of breach, or date range within which breach occurred; (4) date that breach was discovered; (5) clear and concise description of any remediation services offered to affected individuals including toll free numbers and websites to contact credit reporting agencies, remediation service providers, and AG; and (6) clear and concise description of individual’s ability to file or obtain a police report, how to request a security freeze and necessary information to be provide when requesting a security freeze, and that fees may be required to be paid to the consumer reporting agencies.

Notification Recipients

Any affected RI resident. If 500 or more RI residents are affected, must also notify RI AG and credit reporting agencies as to the timing, content, distribution of notices and approx. number of affected individuals. All Dept. of Business Regulation licensees must notify the Dept. of a breach of the security of computerized unencrypted data that poses a significant risk of identity theft.

Attorney General Publishes Breach Data

No.

Private Right of Action Included

No.

Exception to Notification Obligation Exists if the Entity is Complying with Other Laws (HIPPA, GLB, etc.)

Yes, entities subject to and in compliance with (1) the GLB Act, (2) the Federal Interagency Guidance or (3) HIPAA are deemed to be in compliance with this chapter.

Allows Flexibility in Notification Requirements to Entities that Maintain Their Own Notification Procedures Consistent with the Statute

Yes.

Penalties for Violations

Civil penalties up to \$100 per occurrence, or \$200 per occurrence for a knowing and willful violation. AG may bring an action.



Definition of Breach

Unauthorized access to and acquisition of computerized data not rendered unusable through encryption or redaction 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 the resident.

Definition of Personally Identifiable Information

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 neither encrypted nor redacted: (1) SSN; (2) DL number or state ID number; (3) financial account number or credit or debit card number in combination with any required security code, access code or password that would permit access to an individual’s financial account; or (4) 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 will uniquely identify an individual.

Form of Data

Computerized or other data that includes personal identifying information.

Paper Records Covered

No.

Encrypted Data Covered When the Encryption Key Has Been Accessed or Acquired

No.

Entities Covered

A person conducting business in SC that owns, licenses, or maintains computerized data that includes personal information.

Notification Obligation Triggers After Discovery or After Reasonable Investigation

Discovery or notification of the breach, but notification required only 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 the resident.

Time for Notification Once an Obligation is Triggered

If person owns or licenses the personal information, in “the most expedient time possible and without unreasonable delay. If the person maintains the personal information, notification shall be “immediately” following the discovery.

Risk of Harm Trigger for Notification Exists

Yes.

Notification Method

(1) Written notice; (2) Electronic notice, if person’s primary method of communication with the individual is by electronic means or is consistent with the provisions regarding electronic records and signatures in 15 U.S.C. § 7001 and Chapter 6, Title 11 of the 1976 Code; (3) Telephonic notice; or (4) Substitute notice, if the person demonstrates that the cost of providing notice exceeds \$250K or that the affected class of subject persons to be notified exceeds 500,000 or the person has insufficient contact information. Substitute notice consists of: (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.

Mandatory Notification Items

No applicable provision.

Notification Recipients

Any affected resident, or owner or licensee of the personal information if notifier is not owner or licensee.

If required to notify more than 1,000 persons at one time, shall notify, “without unreasonable delay,” the Consumer Protection Division of the Dep’t of Consumer Affairs (through this online portal) and all national consumer reporting agencies (must notify of timing, distribution and content of notice).

Attorney General Publishes Breach Data

No.

Private Right of Action Included

Yes.

Exception to Notification Obligation Exists if the Entity is Complying with Other Laws (HIPPA, GLB, etc.)

Entities subject to and in compliance with the GLB Act or the Federal Interagency Guidance.

Allows Flexibility in Notification Requirements to Entities that Maintain Their Own Notification Procedures Consistent with the Statute

Yes.

Penalties for Violations

Resident injured by a violation of the statute may bring a civil action to recover actual damages (in case of a negligent violation) or damages (in case of willful violation), seek an injunction or recover attorney’s fees and court costs, if successful. Fine of \$1,000 per resident.

South Dakota

S.B. 62

Definition of Breach

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 protection information maintained by the notifier.

Definition of Personally Identifiable Information

(1) SSN; (2) DL number or other unique ID number created or collected by a government body; (3) 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; (4) Health information as defined in 45 CFR 160.103; (5) An ID 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; (6) 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 (7) 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.

Form of Data

Computerized and unencrypted, or computerized and encrypted with the encryption key.

Paper Records Covered

No.

Encrypted Data Covered When the Encryption Key Has Been Accessed or Acquired

Yes, provided that the encryption key that would render the compromised data readable is also subject to breach.

Entities Covered

Any person or business that conducts business in SD that also owns or licenses computerized personal or protected information of SD residents.

Notification Obligation Triggers After Discovery or After Reasonable Investigation

The discovery or notification that a breach has occurred or is reasonably believed to have occurred.

Time for Notification Once an Obligation is Triggered

Within 60 days of discovery or notification of the breach.

Risk of Harm Trigger for Notification Exists

Yes. However, no notification required to individuals if, following appropriate investigation and notice to AG, the notifier reasonably determines that breach will not likely result in harm to affected SD residents. Notifier must document the determination in writing and maintain such documentation for at least 3 years.

Notification Method

(1) Written notice; (2) Electronic notice, if the electronic notice is consistent with 15 U.S.C. § 7001 or if the notifier’s primary method of communication with the SD resident has been by electronic means; or (3) Substitute notice, if the notifier demonstrates that the cost of providing notice would exceed \$250,000, that more than 500,000 people must be notified, or that the notifier lacks sufficient contact information and the notice consists of each of the following: (a) email notice, if the notifier has an email address for the affected individuals; (b) conspicuous posting of the notice on the notifier’s website, if such website exists; and (c) notification to statewide media.

Mandatory Notification Items

No applicable provision.

Notification Recipients

Any SD resident whose personal or protected information was affected by breach, as well as all consumer reporting agencies and any other credit bureau or agency that compiles and maintains files on consumers on a nationwide basis. If more than 250 SD residents must be notified, must also notify AG.

Attorney General Publishes Breach Data

No.

Private Right of Action Included

No.

Exception to Notification Obligation Exists if the Entity is Complying with Other Laws (HIPPA, GLB, etc.)

Yes.

Allows Flexibility in Notification Requirements to Entities that Maintain Their Own Notification Procedures Consistent with the Statute

Yes.

Penalties for Violations

AG may prosecute each failure to disclose as a deceptive act or practice under S.D. Codified Laws § 37-24-6. Additionally, AG may bring action to recover civil penalties of up to \$10,000 per day per violation.



Tennessee

Tenn. Code §§ 47-18-2105 - 2107

Definition of Breach

Acquisition of information (either (i) unencrypted computerized data; (ii) or encrypted computerized data and the encryption key) by an unauthorized person that materially compromises the security, confidentiality, or integrity of personal information maintained by the information holder.

Definition of Personally Identifiable Information

An individual’s first name or first initial and last name in combination with any one or more of the following data elements: (1) SSN; (2) DL 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.

Form of Data

Unencrypted computerized data or encrypted computerized data and the encryption key.

Paper Records Covered

No.

Encrypted Data Covered When the Encryption Key Has Been Accessed or Acquired

Yes, if encryption key is also compromised by breach.

Entities Covered

“Information holder” is defined as any person or business that conducts business in TN, or any TN agency or any of its political subdivisions, that owns or licenses computerized data that includes personal information.

Notification Obligation Triggers After Discovery or After Reasonable Investigation

Discovery or notification of the security breach.

Time for Notification Once an Obligation is Triggered

If information holder owns or licenses personal information, must notify TN resident immediately, but no later than 45 days from discovery or notification of breach. If information holder maintains personal information, must notify owner or licensee of personal information immediately, but no later than 45 days following discovery of the breach.

Risk of Harm Trigger for Notification Exists

No.

Notification Method

(1) Written notice; (2) Electronic notice, if notice provided is consistent with 15 U.S.C. § 7001; or (3) Substitute notice, if the information holder 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 information holder does not have sufficient contact information. Substitute notice shall consist 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 web site page, if the information holder maintains such web site page; and (C) Notification to major statewide media.

Mandatory Notification Items

No applicable provision.

Notification Recipients

Any affected TN resident; data owner, if notifier is not data owner. Must notify all national consumer reporting agencies and credit reporting bureaus if required to notify more than 1,000 TN residents at the same time.

Attorney General Publishes Breach Data

No.

Private Right of Action Included

Yes.

Exception to Notification Obligation Exists if the Entity is Complying with Other Laws (HIPPA, GLB, etc.)

Yes, entities subject to GLB Act or HIPAA are exempt.

Allows Flexibility in Notification Requirements to Entities that Maintain Their Own Notification Procedures Consistent with the Statute

Yes.

Penalties for Violations

Whichever is greater: (i) \$10,000; (ii) \$5,000 per day for each day that a person’s identity has been assumed; or (iii) ten times the amount obtained or attempted to be obtained by the person using the identity theft. Any knowing or willful violation of the terms of an injunction or order issued pursuant to AG action - up to \$5,000 civil penalty for each and every violation of the order recoverable by state, in addition to any other appropriate relief, including, contempt sanctions and awarding of attys’ fees and costs to state for any filings.



Tex. Bus. & Com. Code §§ 521.002, 521.053, 521.151

Definition of Breach

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.

Definition of Personally Identifiable Information

An individual's first name or first initial and last name in combination with any one or more of the following data elements, if the name and the items are not encrypted: (1) SSN; (2) DL number or gov't- issued ID card 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; or information that identifies an individual and relates to (i) the physical or mental health or condition of the individual; (ii) provision of health care to the individual; (iii) payment for the provision of health care to the individual.

Form of Data

Computerized.

Paper Records Covered

No.

Encrypted Data Covered When the Encryption Key Has Been Accessed or Acquired

Yes, if person accessing the data has the key required to decrypt the data.

Entities Covered

A person who conducts business in TX that owns, licenses, or maintains computerized data that contains personal information.

Notification Obligation Triggers After Discovery or After Reasonable Investigation

No.

Time for Notification Once an Obligation is Triggered

If the person owns or licenses personal information, notification shall be "as quickly as possible." If person maintains personal information, notification must be made "immediately" following discovery of the breach.

Risk of Harm Trigger for Notification Exists

No.

Notification Method

(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. Section 7001; or (3) Substitute notice, if the person required to give notice demonstrates that the cost of providing notice would exceed \$250K, the number of affected persons exceeds 500,000, or the person does not have sufficient contact information, the notice may be given by: (a) e-mail, if the person has e-mail addresses for the affected persons; (b) conspicuous posting of the notice on the person's website; or (3) notice published in or broadcast on major statewide media.

Mandatory Notification Items

No applicable provision.

Notification Recipients

Any individual whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person, provided that such individual is a resident of TX or another state that does not require a person to notify the individual of a breach of system security. Must also notify national consumer reporting agencies if notifying more than 10,000 persons at once. In addition, a domestic insurer or HMO should contact its assigned financial analyst at the Texas Department of Insurance if the insurer or HMO experiences or discovers an unauthorized acquisition, release, or use of personal information or sensitive company information.

Attorney General Publishes Breach Data

No.

Private Right of Action Included

No.

Exception to Notification Obligation Exists if the Entity is Complying with Other Laws (HIPPA, GLB, etc.)

No.

Allows Flexibility in Notification Requirements to Entities that Maintain Their Own Notification Procedures Consistent with the Statute

Yes.

Penalties for Violations

AG may bring suit to recover civil penalty of \$2,000 - \$50,000 per violation, and/or action to obtain a TRO or permanent or temporary injunction; AG can also recover expenses including attorney fees. Tex. Bus. & Com. Code § 521.151(a), (f). As amended by S.B. 300, AG may bring suit against a person who fails to take reasonable action to comply with notification requirements for a civil penalty NTE \$100 for each individual to whom notification is due for each consecutive day that the person fails to take reasonable action to comply, NTE \$250K for all individuals to whom notification is due after a single breach.

U.S. Virgin Islands

V.I. Code Ann. Tit. 14 §§ 2208–2212

Definition of Breach

Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the entity.

Definition of Personally Identifiable Information

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 (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.

Form of Data

Computerized and unencrypted.

Paper Records Covered

No.

Encrypted Data Covered When the Encryption Key Has Been Accessed or Acquired

No.

Entities Covered

A person, business, or agency that owns or licenses computerized data that includes personal information.

Notification Obligation Triggers After Discovery or After Reasonable Investigation

The discovery that unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Time for Notification Once an Obligation is Triggered

If data owner, in the most expedient time possible and without unreasonable delay. If only maintaining data, immediately following discovery.

Risk of Harm Trigger for Notification Exists

No.

Notification Method

(1) Written notice; (2) electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code; (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; (B) conspicuous posting of the notice on the website of the person or business, if the person or business maintains one; (C) notification to major territory-wide media.

Mandatory Notification Items

No applicable provision.

Notification Recipients

Any U.S. Virgin Island resident affected by breach.

Attorney General Publishes Breach Data

No.

Private Right of Action Included

Yes.

Exception to Notification Obligation Exists if the Entity is Complying with Other Laws (HIPPA, GLB, etc.)

No.

Allows Flexibility in Notification Requirements to Entities that Maintain Their Own Notification Procedures Consistent with the Statute

Yes.

Penalties for Violations

Any business that violates, proposes to violate, or has violated the data breach notification requirements may be enjoined.

Definition of Breach

Unauthorized acquisition of computerized data maintained by a person that compromises the security, confidentiality, or integrity of personal information.

Definition of Personally Identifiable Information

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 data element is unencrypted or not protected by another method that renders the data unreadable or unusable: (1) SSN; (2) DL number or state ID card number; (3) 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.

Form of Data

Computerized.

Paper Records Covered

No.

Encrypted Data Covered When the Encryption Key Has Been Accessed or Acquired

No.

Entities Covered

A person who owns, licenses, or maintains computerized data that includes UT residents’ personal information.

Notification Obligation Triggers After Discovery or After Reasonable Investigation

When owner or licensee “becomes aware of a breach of system security,” if investigation reveals that misuse of personal information for identity theft or fraud purposes has occurred, or is reasonably likely to occur. If covered entity maintains personal information, but is not owner or licensee, following discovery of breach if misuse of personal information occurs or is reasonably likely to occur.

Time for Notification Once an Obligation is Triggered

If person owns or licenses personal information, notification shall be made “in the most expedient time possible and without unreasonable delay” after investigating scope of breach and restoring reasonable integrity of the system. If person maintains personal information, notification to owner or licensee must be made “immediately” following the discovery of the breach.

Risk of Harm Trigger for Notification Exists

Yes.

Notification Method

(1) By first-class mail to the most recent address the person has for the resident; (2) Electronically, if the person’s primary method of communication with the resident is by electronic means, or if provided in accordance with the consumer disclosure provisions of 15 U.S.C. Section 7001; (3) By telephone, including through the use of automatic dialing technology not prohibited by other law; or (4) by publishing notice of the breach of system security in a newspaper of general circulation and as required by Utah Code § 45-1-101. No substitute notice provisions.

Mandatory Notification Items

No applicable provision.

Notification Recipients

Affected resident, or the owner or licensee of the information if the notifier is not the owner or licensee of the information.

Attorney General Publishes Breach Data

No.

Private Right of Action Included

No.

Exception to Notification Obligation Exists if the Entity is Complying with Other Laws (HIPPA, GLB, etc.)

Yes. Regulated entities that maintain procedures for breach notification pursuant to state or federal law, provided that entity notifies each affected Utah resident in accordance with the other applicable law in the event of a breach

Allows Flexibility in Notification Requirements to Entities that Maintain Their Own Notification Procedures Consistent with the Statute

Yes.

Penalties for Violations

AG may bring suit; fines up to \$2,500 for a single consumer; up to \$100,000 aggregated; injunctive relief.



Vermont

9 Vt. Stat. Ann. §§ 2430, 2435

Definition of Breach

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 maintained by the data collector.

Definition of Personally Identifiable Information

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 protected by another method that renders them unreadable or unusable by unauthorized persons: (1) SSN; (2) Motor vehicle operator’s license number or nondriver ID card number; (3) Financial account number, credit or debit card number, if circumstances exist in which the number could be used without additional identifying information, access codes, or passwords; (4) Account passwords or personal identification numbers or other access codes for a financial account.

Form of Data

Computerized.

Paper Records Covered

No.

Encrypted Data Covered When the Encryption Key Has Been Accessed or Acquired

No.

Entities Covered

Any individual or entity that owns, licenses, maintains, or possesses computerized data that includes personal information concerning a VT resident.

Notification Obligation Triggers After Discovery or After Reasonable Investigation

Following “discovery or notification” of the breach, but notification not required if data collector establishes that misuse of personal information is “not reasonably possible” and data collector provides notice to AG or to department of banking, insurance, securities, and health care administration.

Time for Notification Once an Obligation is Triggered

If data collector owns or licenses personal information, notification shall be made to affected VT resident “in the most expedient time possible and without unreasonable delay, but not later than 45 days after discovery or notification of the breach.” If data collector maintains personal information, notification shall be made “immediately” following discovery of the breach. Must also notify AG or Department of Financial Regulation within 14 business days of discovery of breach or of notification of VT residents, whichever is sooner.

Risk of Harm Trigger for Notification Exists

Yes. However, entities must still notify AG or Dept. of Financial Reg. of breach, even if there is no harm.

Notification Method

(1) Written notice mailed to the consumer’s residence; (2) Electronic notice, for those consumers for whom the data collector has a valid e-mail address if: (I) the data collector does not have consumer’s mailing address or telephone number, 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 provided is consistent with the provisions regarding electronic records and signatures for notices as set forth in 15 U.S.C. § 7001; or (3) Telephonic notice, provided that telephonic contact is made directly with each affected consumer, and the telephonic contact is not through a prerecorded message; or (4) Substitute notice, if the data collector demonstrates that the cost of providing written or telephonic notice would exceed \$5K or that the affected class of affected consumers to be provided written or telephonic notice exceeds 5,000, or the data collector does not have sufficient contact information. Substitute notice shall consist of all of the following: (i) conspicuous posting of the notice on the data collector’s website page if the data collector maintains one; and (ii) notification to major statewide and regional media.

Mandatory Notification Items

Must be clear and conspicuous and contain a description of: (1) the incident in general terms; (2) the type of personal information compromised; (3) the general acts of the business to protect the information from further unauthorized access; (4) a toll-free number to call for further information or assistance; (5) advice that directs the person to remain vigilant by monitoring accounts and free credit reports; and (6) approximate date of the data breach.

Notification Recipients

Any affected VT resident, or owner of data if notifier only maintains or possesses data. Must also notify AG or Dept. of Financial Reg. of number of VT residents affected, and national credit reporting agencies if more than 1,000 consumers affected. All entities regulated by the Dept. of Banking, Insurance, Securities, and Health Care Administration must provide notice to the Dept. within 14 days of discovering any electronic data security breach that compromises a consumer’s non-public personally identifiable information.

Attorney General Publishes Breach Data

Yes.

Private Right of Action Included

No.

Exception to Notification Obligation Exists if the Entity is Complying with Other Laws (HIPPA, GLB, etc.)

Entities subject to (1) Federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and (2) NCUA Customer Notice or Final Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice are exempt.

Allows Flexibility in Notification Requirements to Entities that Maintain Their Own Notification Procedures Consistent with the Statute

No.

Penalties for Violations

AG or Dept. of Financial Reg. may investigate, prosecute, and obtain remedies for violations of statute.

Virginia

Va. Code Ann. § 18.2-186.6; § 32.1 - 127.1:05

Definition of Breach

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 Virginia.

Definition of Personally Identifiable Information

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 neither encrypted nor redacted: (1) SSN; (2) driver’s license number or state ID number issued in lieu of a driver’s license number; (3) financial account number, or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a resident’s financial accounts.

Form of Data

Computerized.

Paper Records Covered

No.

Encrypted Data Covered When the Encryption Key Has Been Accessed or Acquired

Yes, if encrypted information is accessed and acquired in an unencrypted form or if the security breach involves a person with access to the encryption key and the individual or entity reasonably believes that such breach has caused or will cause identity theft or other fraud to any VA resident.

Entities Covered

An individual or entity that owns, licenses or maintains computerized data that includes personal information of a VA resident.

Notification Obligation Triggers After Discovery or After Reasonable Investigation

Notification or discovery of breach, but notification only required if information that was, or reasonably believed to have been, accessed and acquired causes, or the individual or entity reasonably believes it has caused or will cause, identity theft or another fraud to any resident of VA.

Time for Notification Once an Obligation is Triggered

Without unreasonable delay.

Risk of Harm Trigger for Notification Exists

Yes, must cause or reasonably believed to have caused or will cause identity theft or other fraud.

Notification Method

(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 \$50K, 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. 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.

Mandatory Notification Items

Notice must include: (1) description of incident in general terms; (2) type of personal information obtained as a result of the breach; (3) general acts of entity to protect personal info from further unauthorized access; (4) telephone number that person may call for further information and assistance, and (5) advice directing person to remain vigilant by reviewing account statements and monitoring free credit reports.

Notification Recipients

Affected VA residents and AG. If not data owner or licensee, must notify owner or licensee. If more than 1,000 residents notified, must notify AG and nationwide consumer reporting agencies of the timing, distribution, and content of the notice. Income tax preparers who discover unauthorized access and acquisition of unencrypted and unredacted tax return information that compromises the confidentiality of the information must notify the Department of Taxation without unreasonable delay.

Attorney General Publishes Breach Data

No.

Private Right of Action Included

Yes.

Exception to Notification Obligation Exists if the Entity is Complying with Other Laws (HIPPA, GLB, etc.)

Yes. Entities regulated by GLB Act or entities that comply with notification requirements pursuant to rules or regulations established by entity’s primary state or federal regulator.

Allows Flexibility in Notification Requirements to Entities that Maintain Their Own Notification Procedures Consistent with the Statute

Yes.

Penalties for Violations

AG may bring action, not to exceed \$150K per breach of the security of the system or a series of breaches of a similar nature that are discovered in a single investigation. Individuals may recover direct personal economic damages.

Miscellaneous Provisions

Any signed income tax preparer must notify the Dept. of Taxation without unreasonable delay after the discovery or notification of unauthorized access and acquisition of unencrypted and unredacted return information that compromises the confidentiality of such information maintained by such signing income tax return preparer and that creates a reasonable belief that an unencrypted and unredacted version of such information was accessed and acquired by an unauthorized person and that causes, or such is reasonably believed has caused or will cause, identity theft or other fraud. Such notification must include name and taxpayer ID number of any taxpayer that may be affected by any such breach of security, as well as the name and tax ID number of the income tax return preparer, and such other information as the Dept. may prescribe.

Washington

Wash. Rev. Code §§ 19.255.010–.020;
§§ 42.56.010; §§ 42.56.590

Definition of Breach

Unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Breach of secured personal information must be disclosed if 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.

Definition of Personally Identifiable Information

An individual’s first name or first initial and last name in combination with any one or more of the following data elements: (1) SSN; (2) driver’s license number or WA ID card 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.

Form of Data

All data.

Paper Records Covered

Yes.

Encrypted Data Covered When the Encryption Key Has Been Accessed or Acquired

Yes, notice is required if information acquired and accessed is not secured during a breach or if the confidential process, encryption key or other means to decipher the secured information was acquired by an unauthorized person.

Entities Covered

Any person that conducts business in WA that owns, licenses, or maintains any data (computerized or hard copy) that includes personal information.

Notification Obligation Triggers After Discovery or After Reasonable Investigation

After discovery or notification of breach, but no notification required if breach is not reasonably likely to subject consumers to a risk of harm.

Time for Notification Once an Obligation is Triggered

If person owns or licenses personal data, notification to WA residents and AG (if required) must be in the most expedient time possible and without delay, but no more than 45 calendar days after breach was discovered. If the person maintains the personal information, notification is required immediately after the breach.

Risk of Harm Trigger for Notification Exists

Yes. Must be reasonably likely to subject consumers to a risk of harm.

Notification Method

(1) Written notice; (2) Electronic notice, if notice provided is consistent with provisions re electronic records and signatures set forth in 15 U.S.C. Sec. 7001; or (3) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed \$250K 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 (A) E-mail if person or business has an e-mail address for the affected person, (B) Conspicuous posting of the notice on web site page of person or business, if web site page is maintained, and (C) Notification to major statewide media.

Mandatory Notification Items

Any person or business that is required to issue notification shall meet all of the following requirements: (a) notification must be written in plain language; (b) notification must include, at a minimum, the following information: (i) the name and contact information of the reporting person or business subject to this law; (ii) a list of the types of personal information that were or are reasonably believed to have been the subject of a breach; and (iii) the toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed personal information.

Notification Recipients

Affected resident, or owner or licensee of the information if notifier is not the owner or licensee. Any person or business that is required to notify more than 500 WA residents as a result of a single breach shall, by the time notice is provided to affected consumers, electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the AG. The person or business shall also provide to the AG, the number of WA consumers affected by the breach, or an estimate if the exact number is not known. Covered Entities as defined under HIPAA shall notify the AG in compliance with notification requirements under Section 13402 of HITECH. Financial institutions must notify the AG. Insurance licensees must notify the insurance commissioner about the number of consumers potentially affected and what actions are being taken, in writing, within two business days after determining notification must be sent to consumers.

Attorney General Publishes Breach Data

Yes.

Private Right of Action Included

Yes.

Exception to Notification Obligation Exists if the Entity is Complying with Other Laws (HIPPA, GLB, etc.)

Entities under HIPAA are deemed to have complied with this law with respect to PHI if it has complied with Section 13402 of HITECH. Financial institutions under the authority of the office of the comptroller of the currency, the FDIC, the national credit union administration, or the federal reserve system are deemed to have complied with the requirements of this section with respect to “sensitive customer information,” if the financial institution provides notice to affected consumers pursuant to the interagency guidelines and the notice complies with the customer notice provisions of the interagency guidelines establishing information security standards and the interagency guidance on response program for unauthorized access to customer information and customer notice under 12 CFR Part 364.

Allows Flexibility in Notification Requirements to Entities that Maintain Their Own Notification Procedures Consistent with the Statute

Yes.

Penalties for Violations

Private right of action for any affected consumer. Any person or business that violates, proposes to violate or has violated the data breach law may be enjoined. AG may bring an action on behalf of state or WA residents affected by breach.

West Virginia

W. Va. Code § 46A-2A-101 - 105

Definition of Breach

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.

Definition of Personally Identifiable Information

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) SSN; (B) Driver's license number or state ID 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, access code or password that would permit access to a resident's financial accounts.

Form of Data

Computerized.

Paper Records Covered

No.

Encrypted Data Covered When the Encryption Key Has Been Accessed or Acquired

Yes, if encrypted information is accessed and acquired in an unencrypted form or if 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 WV resident.

Entities Covered

Any individual or entity that owns, licenses, or maintains computerized data that includes personal information.

Notification Obligation Triggers After Discovery or After Reasonable Investigation

Discovery or notification of security breach, and that causes, or the individual or entity reasonably believes has caused or will cause, identity theft or other fraud to any resident of WV.

Time for Notification Once an Obligation is Triggered

Without unreasonable delay and as soon as practicable if notifying data owner.

Risk of Harm Trigger for Notification Exists

Yes. Must have caused or will cause identity theft or other fraud to any resident of this state.

Notification Method

(1) Written notice; (2) Telephonic notice; (3) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures, set forth in Section 7001, United States Code Title 15, Electronic Signatures in Global and National Commerce Act.; or (4) Substitute notice, if the individual or the entity demonstrates that the cost of providing notice will exceed \$50K or that the affected class of residents to be notified exceeds 100,000 persons or that the individual or the entity does not have sufficient contact information or to provide notice. Substitute notice shall consist 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.

Mandatory Notification Items

Description of categories of information breached, including elements of personal information believed to have been breached; (2) Phone number or website address that individuals may contact to learn: (a) types of info entity maintained about individual or individuals in general; and (b) whether or not entity maintained info about that individual, and (3) toll-free contact numbers and addresses for credit agencies and information on how to place a fraud alert or security freeze.

Notification Recipients

Any affected WV resident, or owner or licensee of the information if notifier is not the owner or licensee. Must also notify all nationwide consumer reporting agencies if more than 1,000 WV residents need to be notified (not applicable to entities subject to GLB Act).

Attorney General Publishes Breach Data

No.

Private Right of Action Included

No.

Exception to Notification Obligation Exists if the Entity is Complying with Other Laws (HIPPA, GLB, etc.)

(1) Financial institution in compliance with Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice; (2) entity that complies with the notification requirements or procedures pursuant to the rules, regulation, procedures or guidelines established by the entity's primary or functional regulator.

Allows Flexibility in Notification Requirements to Entities that Maintain Their Own Notification Procedures Consistent with the Statute

Yes.

Penalties for Violations

AG may bring an enforcement action; civil penalty NTE \$150,000 per breach of security of the system or series of breaches of a similar nature that are discovered in a single investigation. Violation by a licensed financial institution shall be enforceable exclusively by the financial institution's primary functional regulator.



Definition of Breach

Acquisition by a person whom the entity that maintains, licenses, or stores personal information in WI and is not authorized to acquire the personal information.

Definition of Personally Identifiable Information

An individual’s last name and first name or first initial, in combination with and linked to any of the following elements: (1) SSN; (2) driver’s license number or state ID card 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 the individual’s financial account; (4) DNA profile; and (5) unique biometric data including fingerprint, voice print, retina or iris image or any other unique physical representation.

Form of Data

All data.

Paper Records Covered

Yes.

Encrypted Data Covered When the Encryption Key Has Been Accessed or Acquired

No.

Entities Covered

Individual or entity that owns, maintains or stores personal information in WI, including entities that: (i) conduct business in WI and maintain personal information in the ordinary course of business, (ii) license personal information in WI; (iii) maintain a depository account for a WI resident; or (iv) lend money to a WI resident.

Notification Obligation Triggers After Discovery or After Reasonable Investigation

If entity knows that personal information in the entity’s possession has been acquired by an unauthorized person, but notice not required if acquisition of personal information does not create a material risk of identity theft or fraud to the subject of the personal information.

Time for Notification Once an Obligation is Triggered

Within a reasonable time, not to exceed 45 days. If notifying data owner, as soon as practicable.

Risk of Harm Trigger for Notification Exists

Yes.

Notification Method

By mail or method the entity has previously used to communicate with the resident. If the entity cannot with reasonable diligence determine the mailing addresses, notice by a method reasonably calculated to reach the resident is acceptable.

Mandatory Notification Items

Must indicate that the entity knows of the unauthorized acquisition. Upon written request of an affected resident, the entity shall identify the personal information that was acquired.

Notification Recipients

Any affected WI resident, or owner or licensee of the personal information if notifier is not the owner or licensee. Must also notify, without unreasonable delay, all consumer reporting agencies if more than 1,000 WI residents are to be notified. All licensed insurers must notify the Insurance Commissioner of any unauthorized access to personal information of WI residents.

Attorney General Publishes Breach Data

No.

Private Right of Action Included

No.

Exception to Notification Obligation Exists if the Entity is Complying with Other Laws (HIPPA, GLB, etc.)

Entities in compliance with GLB Act or the HHS Privacy Rule.

Allows Flexibility in Notification Requirements to Entities that Maintain Their Own Notification Procedures Consistent with the Statute

No.

Penalties for Violations

No applicable provision.



Wyoming

Wyo. Stat. §§ 40-12-501 et seq.

Definition of Breach

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.

Definition of Personally Identifiable Information

Aan individual's first name or first initial and last name in combination with one or more of the following data elements, when the following data elements are not redacted: (1) Address; (2) Telephone number; (3) SSN; (4) Driver's license number; (5) Account number, credit or debit card number, in combination with any security code, access code or password that would permit access to an individual's financial account; (6) Tribal ID card; or (7) Federal or state government issued identification card; (8) Shared secrets or security tokens that are known to be used for data based authentication; (9) A username or email address, in combination with a password or security question and answer that would permit access to an online account; (10) A birth or marriage certificate; (11) Medical information, meaning a person's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; (12) 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; (13) Unique biometric data, meaning data generated from measurements or analysis of human body characteristics for authentication purposes; (14) An individual taxpayer identification number.

Form of Data

Computerized.

Paper Records Covered

No.

Encrypted Data Covered When the Encryption Key Has Been Accessed or Acquired

Only applies to non-"redacted" data, with redaction defined as alteration or truncation of data such that no more than 5 digits of the data defined as "personal identifying information" is accessible.

Entities Covered

An individual or commercial entity that conducts business in WY and that owns, maintains, or licenses computerized personal information.

Notification Obligation Triggers After Discovery or After Reasonable Investigation

As soon as individual or commercial entity becomes aware of a breach, shall conduct a reasonable and prompt investigation to determine likelihood that personal information has been or will be misused.

Time for Notification Once an Obligation is Triggered

If person or entity owns or licenses personal information, notification shall be made as soon as possible, and in the most expedient time possible and without unreasonable delay. If person or entity only maintains personal information, notification shall be made as soon as practicable after discovery of the breach.

Risk of Harm Trigger for Notification Exists

Yes.

Notification Method

(1) Written notice; (2) E-mail notice; or (3) Substitute notice, if person demonstrates that the cost of providing notice would exceed \$10K (for Wyoming-based businesses) or \$250K (for businesses operating, but not based, in Wyoming), affected class of persons is larger than 10,000 persons (for Wyoming-based businesses) or 500,000 persons (for non-Wyoming based businesses), or person does not have sufficient contact information. Substitute notice shall consist of: (A) Conspicuous posting of the notice on the Internet, 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. The notice to media shall include a toll-free phone number where an individual can learn whether or not that individual's personal data is included in the security breach. 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.

Mandatory Notification Items

Notice shall be clear and conspicuous and shall include, at a minimum : (i) A toll-free number that the individual may use to contact the person collecting the data and 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.

Notification Recipients

Any affected resident, or the business entity for which information was maintained if notifier only maintains personal information on behalf of another person or entity.

Attorney General Publishes Breach Data

No.

Private Right of Action Included

No.

Exception to Notification Obligation Exists if the Entity is Complying with Other Laws (HIPPA, GLB, etc.)

Yes, any financial institution or federal credit union that maintains notification procedures subject to the requirements of the GLB Act, is deemed to be in compliance with this section if the financial institution or federal credit union notifies affected WY residents in compliance with the requirements of the GLB Act.

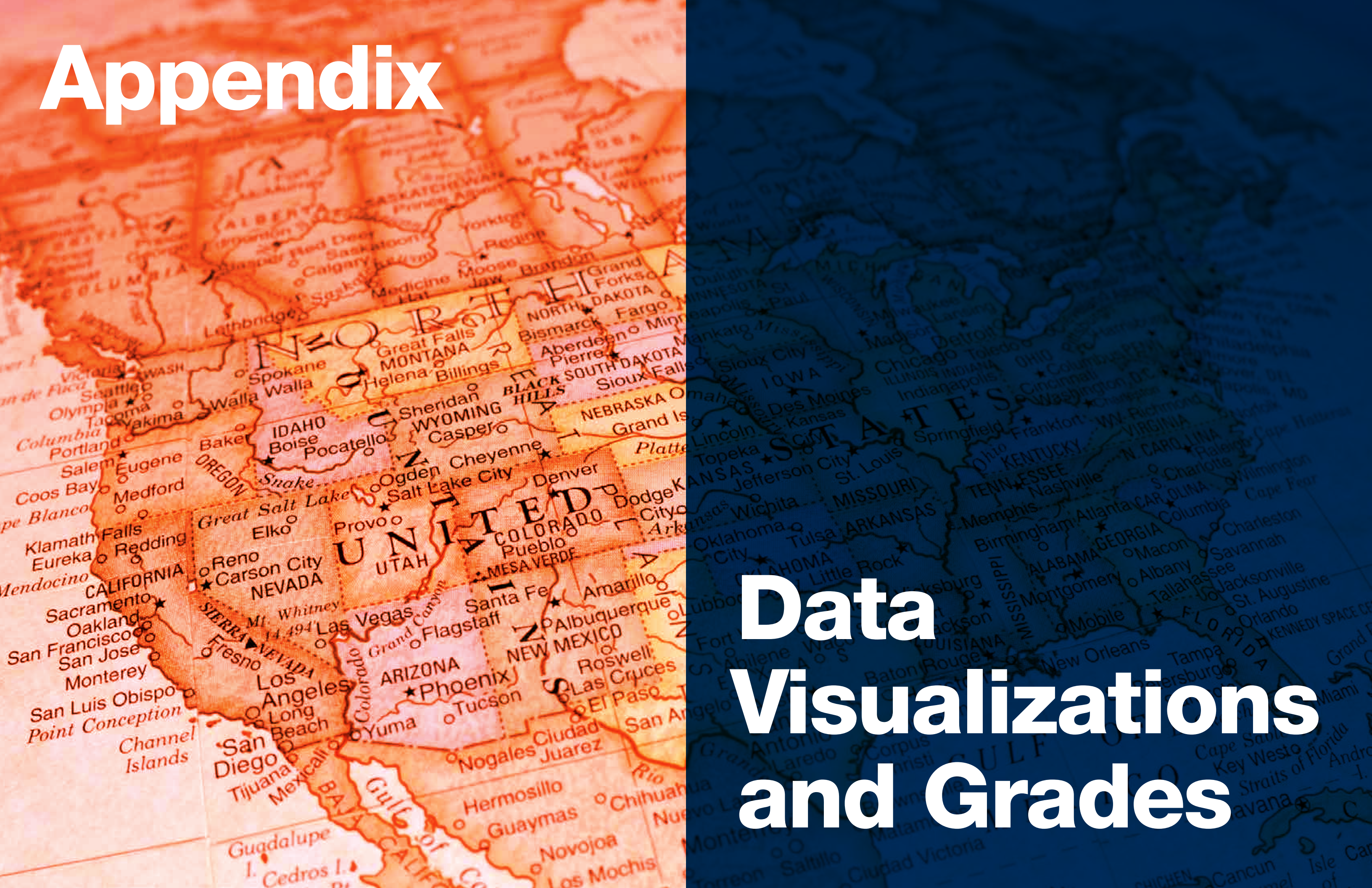
Allows Flexibility in Notification Requirements to Entities that Maintain Their Own Notification Procedures Consistent with the Statute

No.

Penalties for Violations

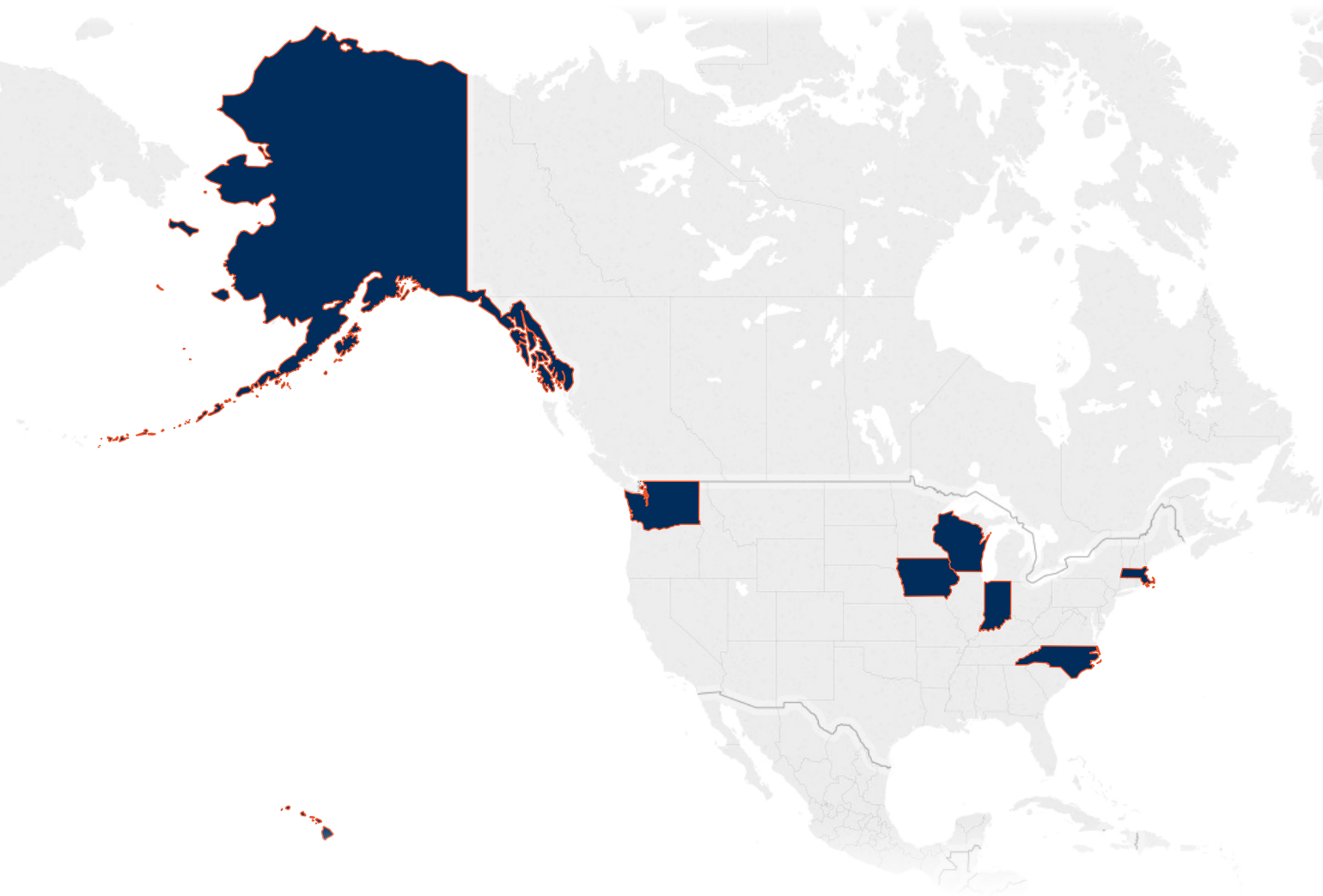
AG may bring an action in law or equity to ensure compliance, to recover damages, or both.

Appendix



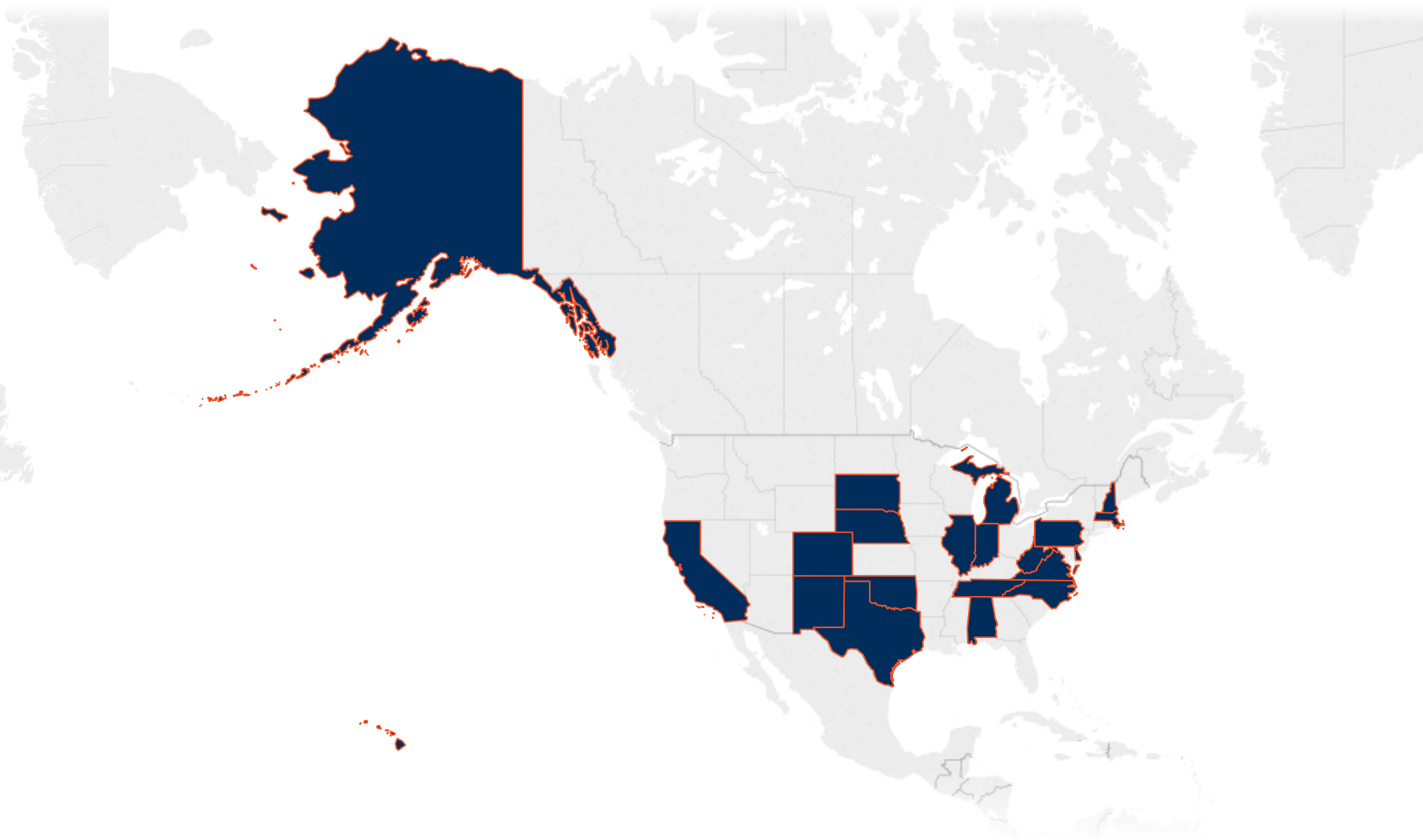
Data Visualizations and Grades

States Covering Paper Records



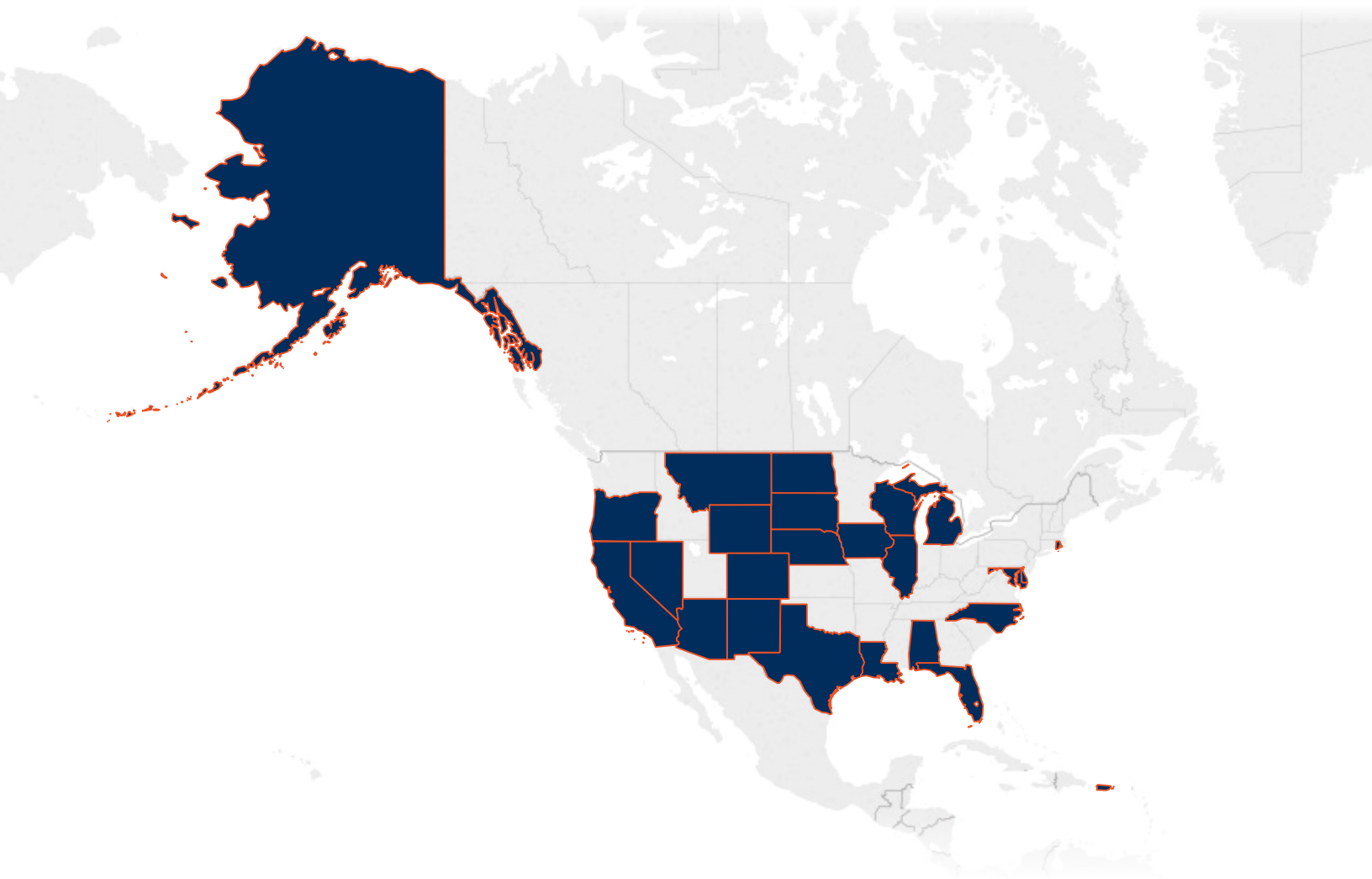
- | | | |
|---------|----------------|------------|
| Alaska | Iowa | Washington |
| Hawaii | Massachusetts | Wisconsin |
| Indiana | North Carolina | |

States Requiring Notification When Both Encrypted Data and the Encryption Key are Exposed



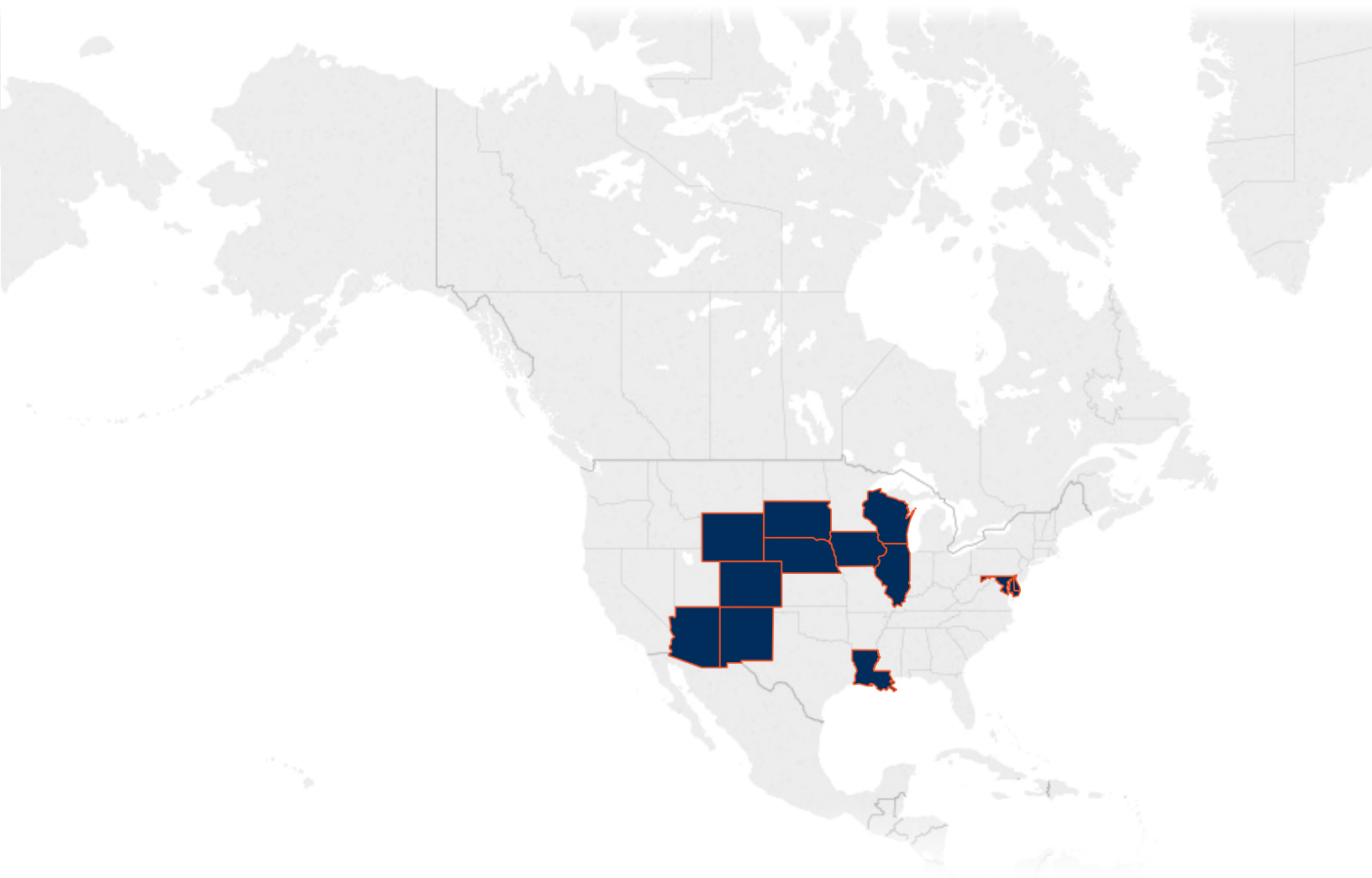
- | | | | | |
|------------|----------|---------------|----------------|---------------|
| Alabama | Delaware | Massachusetts | New Mexico | South Dakota |
| Alaska | Hawaii | Michigan | North Carolina | Tennessee |
| California | Illinois | Nebraska | Oklahoma | Texas |
| Colorado | Indiana | New Hampshire | Pennsylvania | Virginia |
| | | | | West Virginia |

States and Territories with Personal Information Definition Including Medical Information



- | | | | | |
|------------|-----------|----------|----------------|--------------|
| Alabama | Delaware | Maryland | New Mexico | Rhode Island |
| Alaska | Florida | Michigan | North Dakota | South Dakota |
| Arizona | Illinois | Montana | North Carolina | Texas |
| California | Iowa | Nebraska | Oregon | Wisconsin |
| Colorado | Louisiana | Nevada | Puerto Rico | Wyoming |

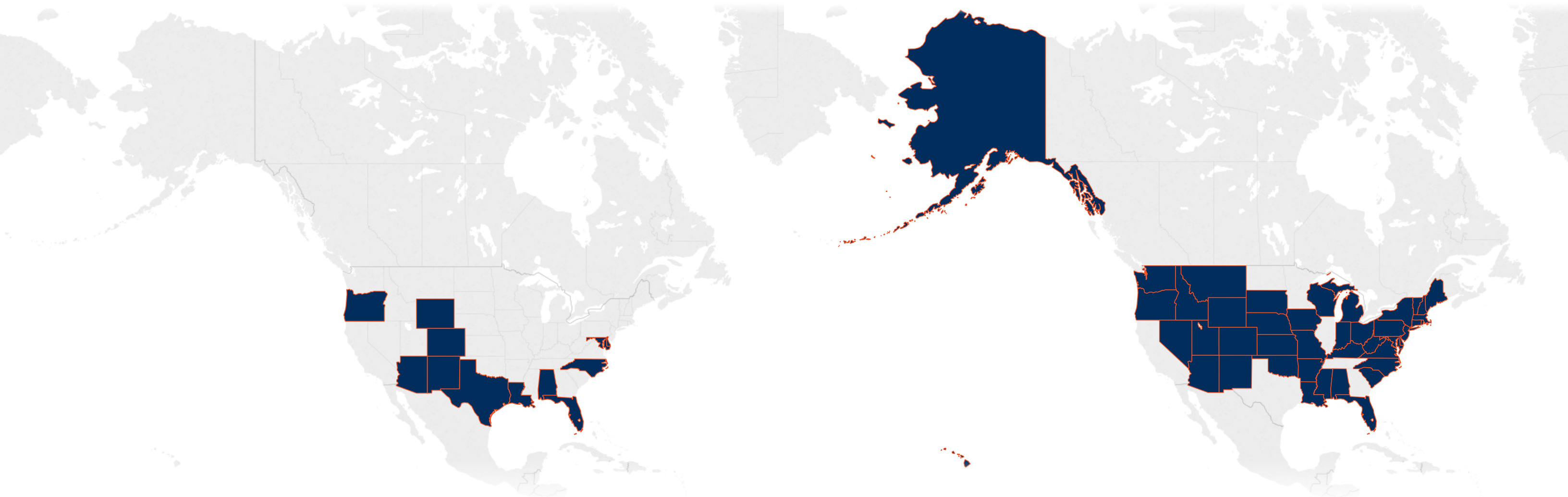
States with Personal Information Definition Including Biometric Information



- | | | |
|----------|-----------|--------------|
| Arizona | Illinois | New Mexico |
| Colorado | Louisiana | South Dakota |
| Delaware | Maryland | Wisconsin |
| Iowa | Nebraska | Wyoming |

States with
Personal Information Definition
Including Passport Information

States and Territories Allowing a
Breached Entity to Avoid Notifying if
it Determines There is *No Reasonable
Likelihood of Harm* to Residents

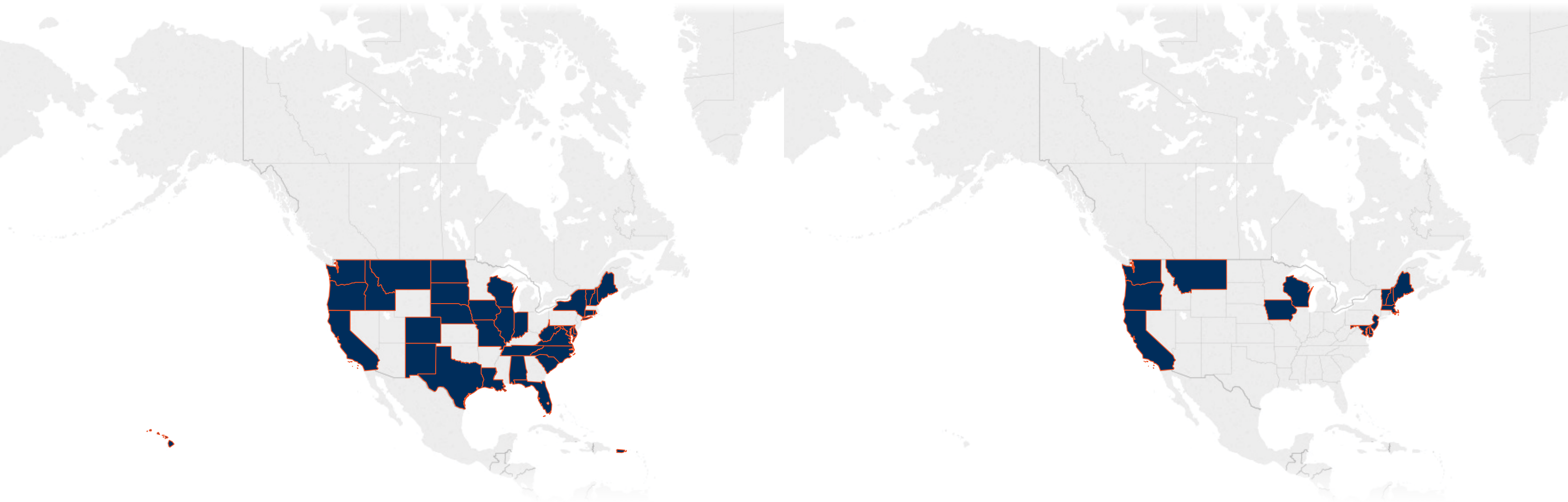


- Alabama
- Arizona
- Colorado
- Delaware
- Florida
- Louisiana
- Maryland
- North Carolina
- Oregon
- New Mexico
- Texas
- Wyoming

- Alabama
- Alaska
- Arizona
- Arkansas
- Colorado
- Connecticut
- Delaware
- Florida
- Guam
- Hawaii
- Idaho
- Indiana
- Iowa
- Kansas
- Kentucky
- Louisiana
- Maine
- Maryland
- Massachusetts
- Michigan
- Mississippi
- Missouri
- Montana
- Nebraska
- Nevada
- New Hampshire
- New Jersey
- New York
- North Carolina
- Ohio
- Oklahoma
- Oregon
- Pennsylvania
- Rhode Island
- South Carolina
- South Dakota
- Utah
- Vermont
- Virginia
- Washington
- West Virginia
- Wisconsin
- Wyoming

States and Territories Requiring Notification to the Attorney General

States in Which the Attorney General Publishes Breach Data

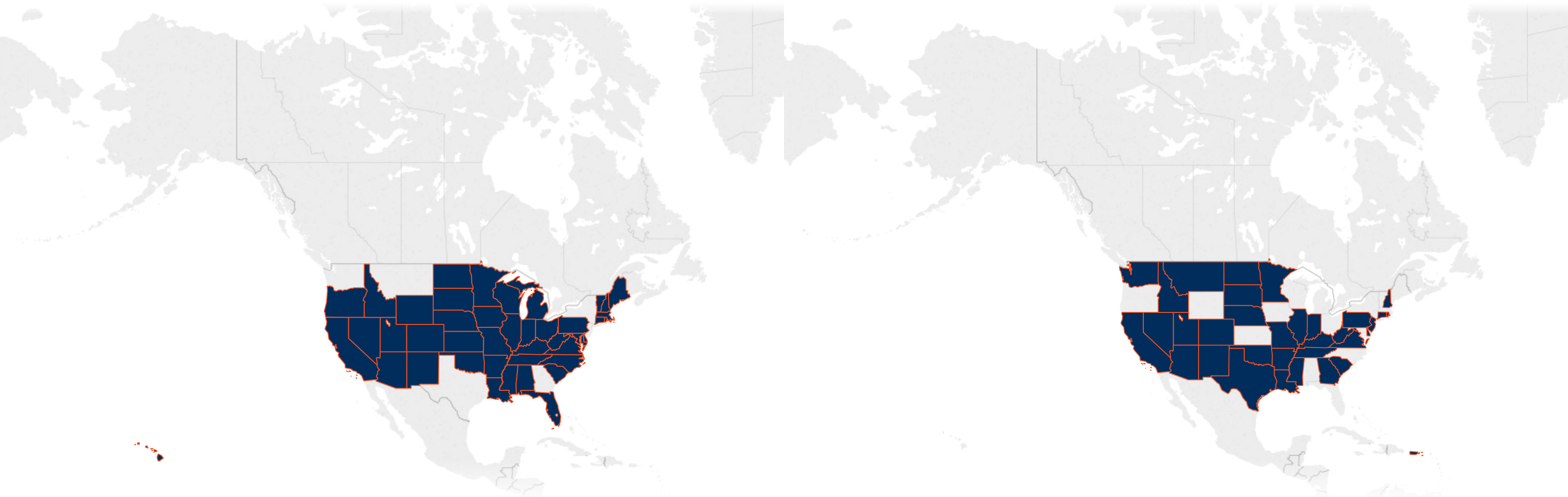


- Alabama
California
Colorado
Connecticut
Delaware
Florida
Hawaii
Idaho
Illinois
- Indiana
Iowa
Louisiana
Missouri
Nebraska
New Hampshire
New Mexico
New York
North Dakota
- North Carolina
Maine
Maryland
Montana
Oregon
Puerto Rico
Rhode Island
South Carolina
South Dakota
- Tennessee
Texas
Vermont
Virginia
Washington
West Virginia
Wisconsin

- California
Delaware
Iowa
Maine
Maryland
- Massachusetts
Montana
New Hampshire
New Jersey
Oregon
- Vermont
Washington
Wisconsin

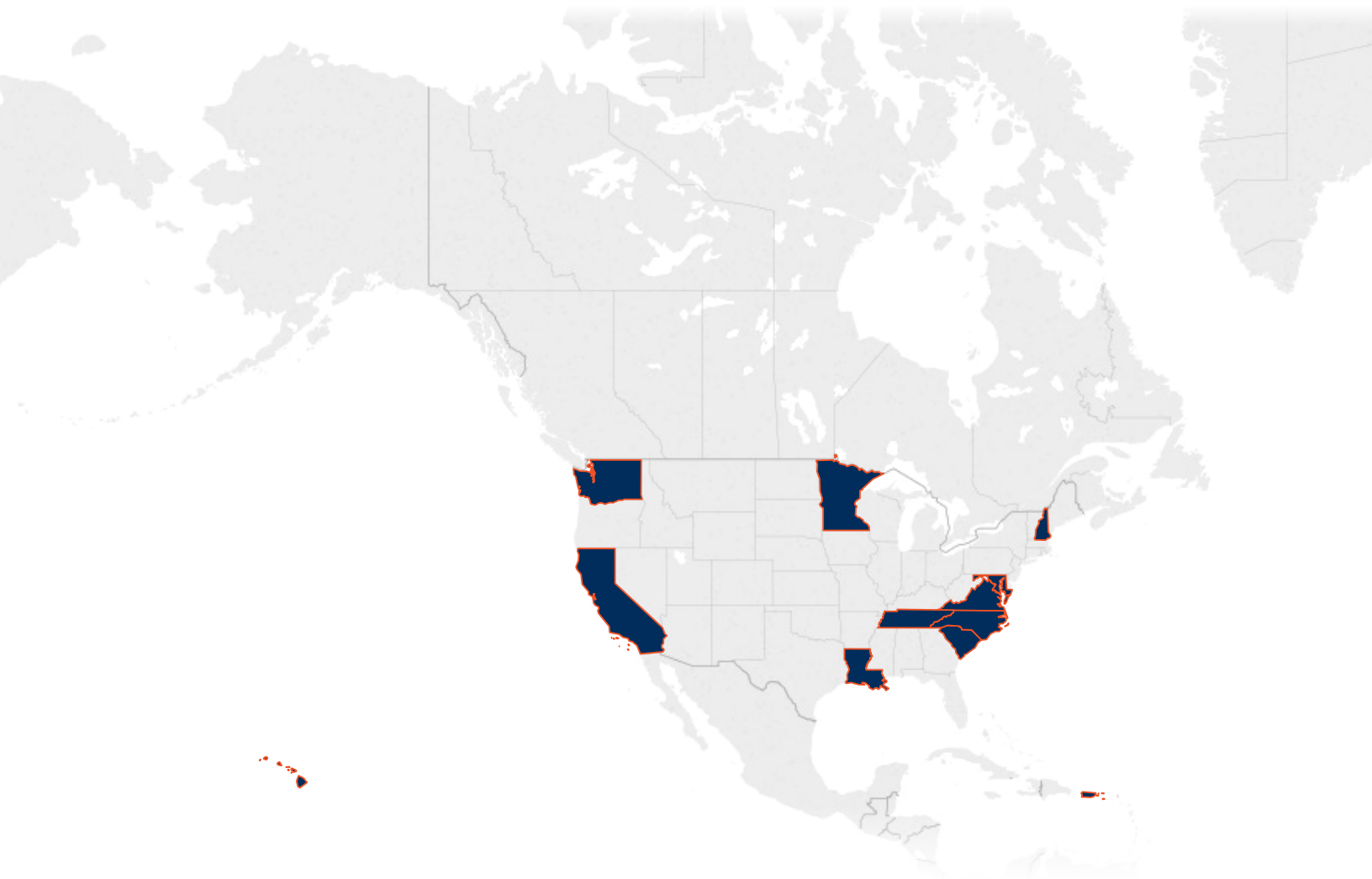
States and Territories Exempting Entities from the Notification Statute if the Entity is Complying with Other Federal Laws with Notification Requirements (such as HIPAA, GLB, etc.)

States and Territories Allowing Flexibility in Notification Requirements to Entities that Maintain Their Own Notification Procedures Consistent with the State Statute



Alabama	Guam	Maine	New Hampshire	South Carolina	Arkansas	Idaho	Nevada	Rhode Island
Arkansas	Hawaii	Maryland	New Mexico	South Dakota	Arizona	Indiana	New Hampshire	South Dakota
Arizona	Idaho	Massachusetts	North Carolina	Tennessee	California	Kentucky	New Jersey	Tennessee
California	Illinois	Michigan	North Dakota	Utah	Colorado	Louisiana	New Mexico	Texas
Colorado	Indiana	Minnesota	Ohio	Vermont	Connecticut	Minnesota	North Dakota	Utah
Connecticut	Iowa	Mississippi	Oklahoma	Virginia	District of Columbia	Mississippi	Oklahoma	Virginia
District of Columbia	Kansas	Missouri	Oregon	West Virginia	Delaware	Missouri	Pennsylvania	Washington
Delaware	Kentucky	Nebraska	Pennsylvania	Wisconsin	Georgia	Montana	Puerto Rico	West Virginia
Florida	Louisiana	Nevada	Rhode Island	Wyoming	Guam	Nebraska	South Carolina	

States and Territories in Which Individuals Have a Private Right of Action



California
District of Columbia
Hawaii
Louisiana
Maryland

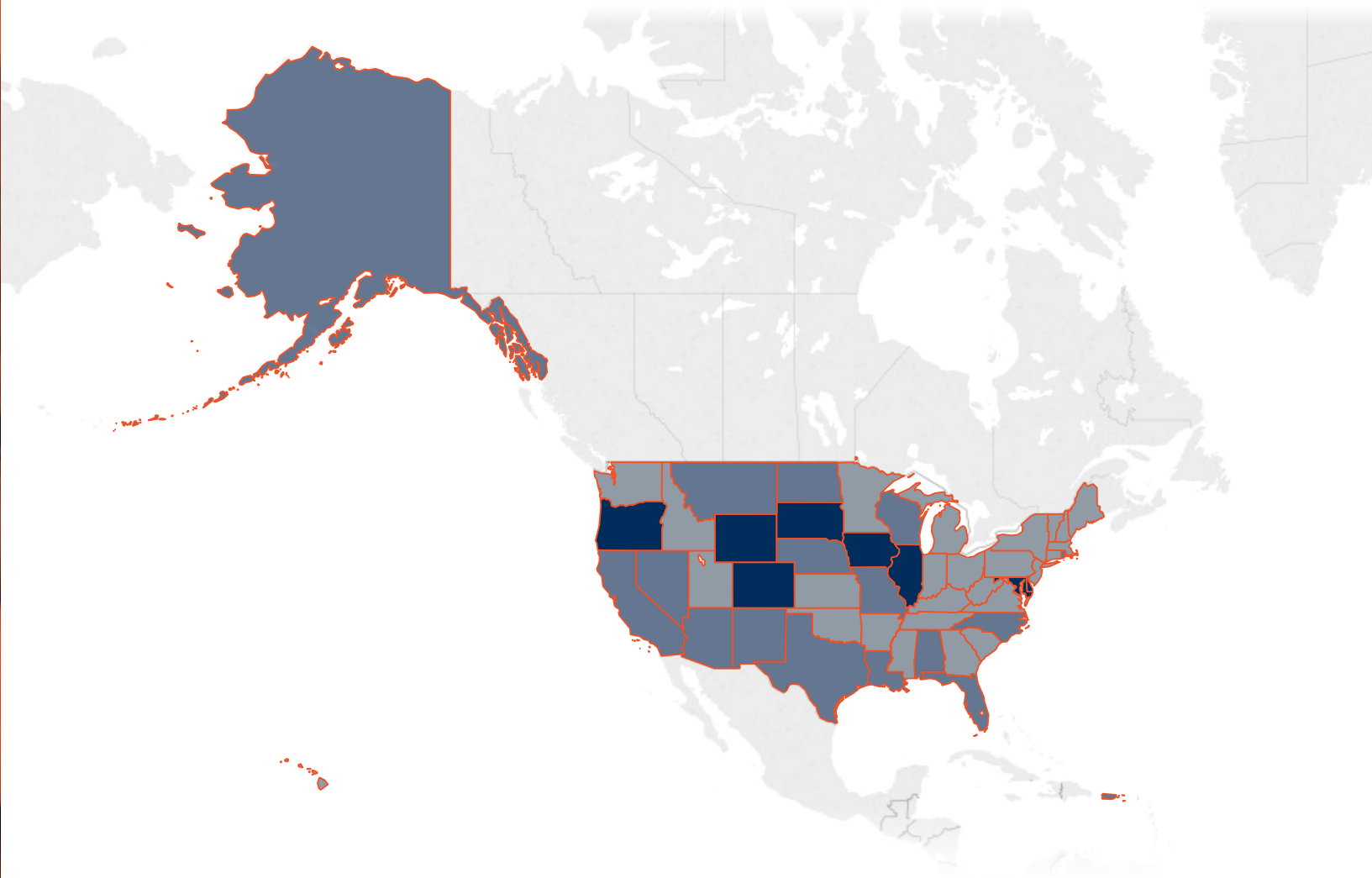
Minnesota
New Hampshire
North Carolina
South Carolina
Tennessee

Puerto Rico
Virginia
Washington



Grading State and Territory Definitions of Personal Information

Alabama	Florida	Kentucky	Montana	Ohio	Texas
Alaska	Georgia	Louisiana	Nebraska	Oklahoma	U.S. Virgin Islands
Arizona	Guam	Maine	Nevada	Oregon	Utah
Arkansas	Hawaii	Maryland	New Hampshire	Pennsylvania	Vermont
California	Idaho	Massachusetts	New Jersey	Puerto Rico	Virginia
Colorado	Illinois	Michigan	New Mexico	Rhode Island	Washington
Connecticut	Indiana	Minnesota	New York	South Carolina	West Virginia
Delaware	Iowa	Mississippi	North Carolina	South Dakota	Wisconsin
District of Columbia	Kansas	Missouri	North Dakota	Tennessee	Wyoming



Has an expanded definition, including biometric data and medical data.

A

Has an expanded definition, including biometric data, or medical data, but not both.

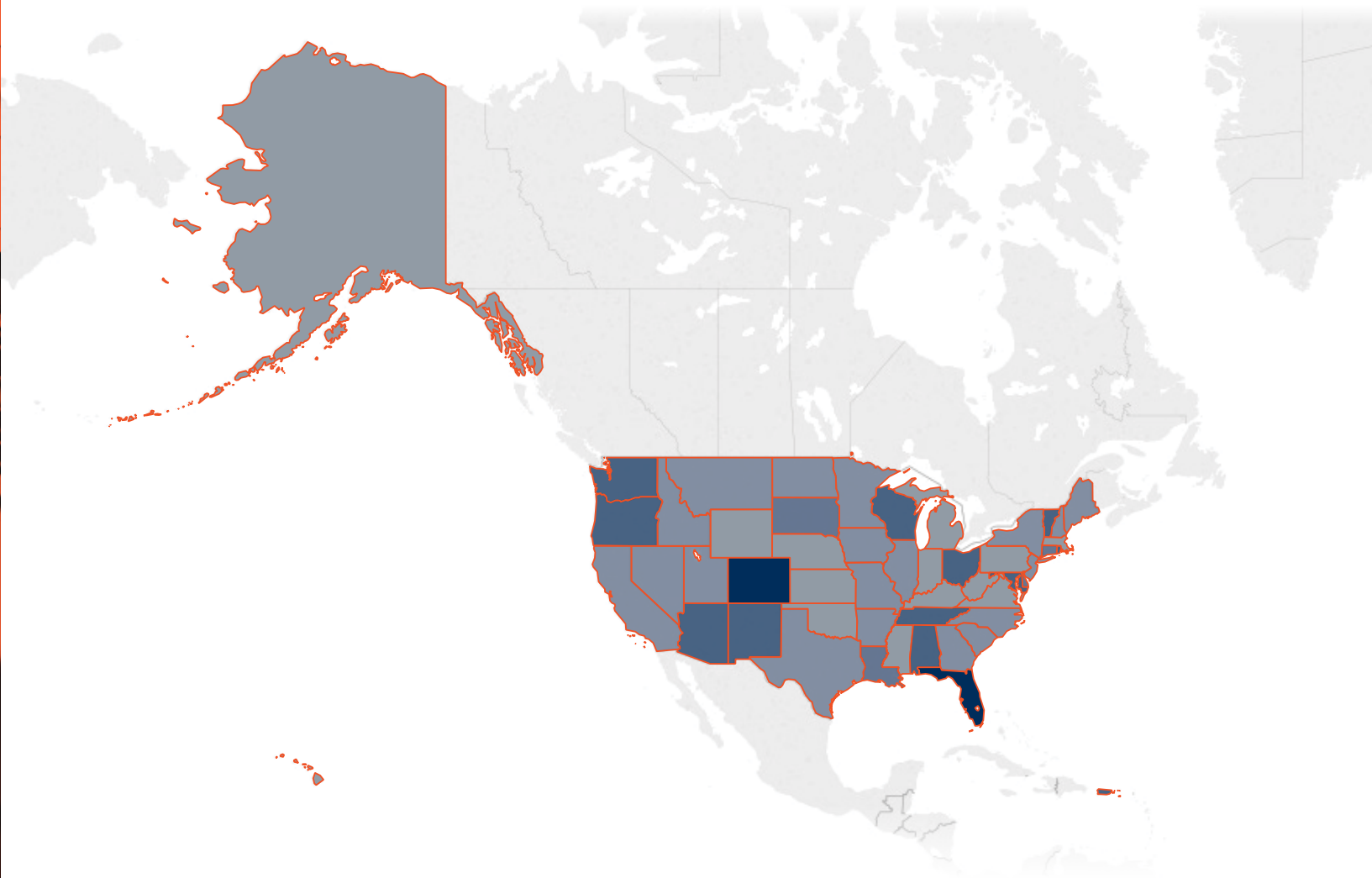
B

Baseline definition of personal information.

C

Grading State and Territory Notification Deadlines

Alabama	Florida	Kentucky	Montana	Ohio	Texas
Alaska	Georgia	Louisiana	Nebraska	Oklahoma	U.S. Virgin Islands
Arizona	Guam	Maine	Nevada	Oregon	Utah
Arkansas	Hawaii	Maryland	New Hampshire	Pennsylvania	Vermont
California	Idaho	Massachusetts	New Jersey	Puerto Rico	Virginia
Colorado	Illinois	Michigan	New Mexico	Rhode Island	Washington
Connecticut	Indiana	Minnesota	New York	South Carolina	West Virginia
Delaware	Iowa	Mississippi	North Carolina	South Dakota	Wisconsin
District of Columbia	Kansas	Missouri	North Dakota	Tennessee	Wyoming



Requires notification within 30 days of obligation triggering.

A

Requires notification within 45 days of obligation triggering.

B

Requires notification within 60 or 90 days of obligation triggering.

C

Has limited reporting requirements depending on the category of data, or mandates notification after discovery of breach.

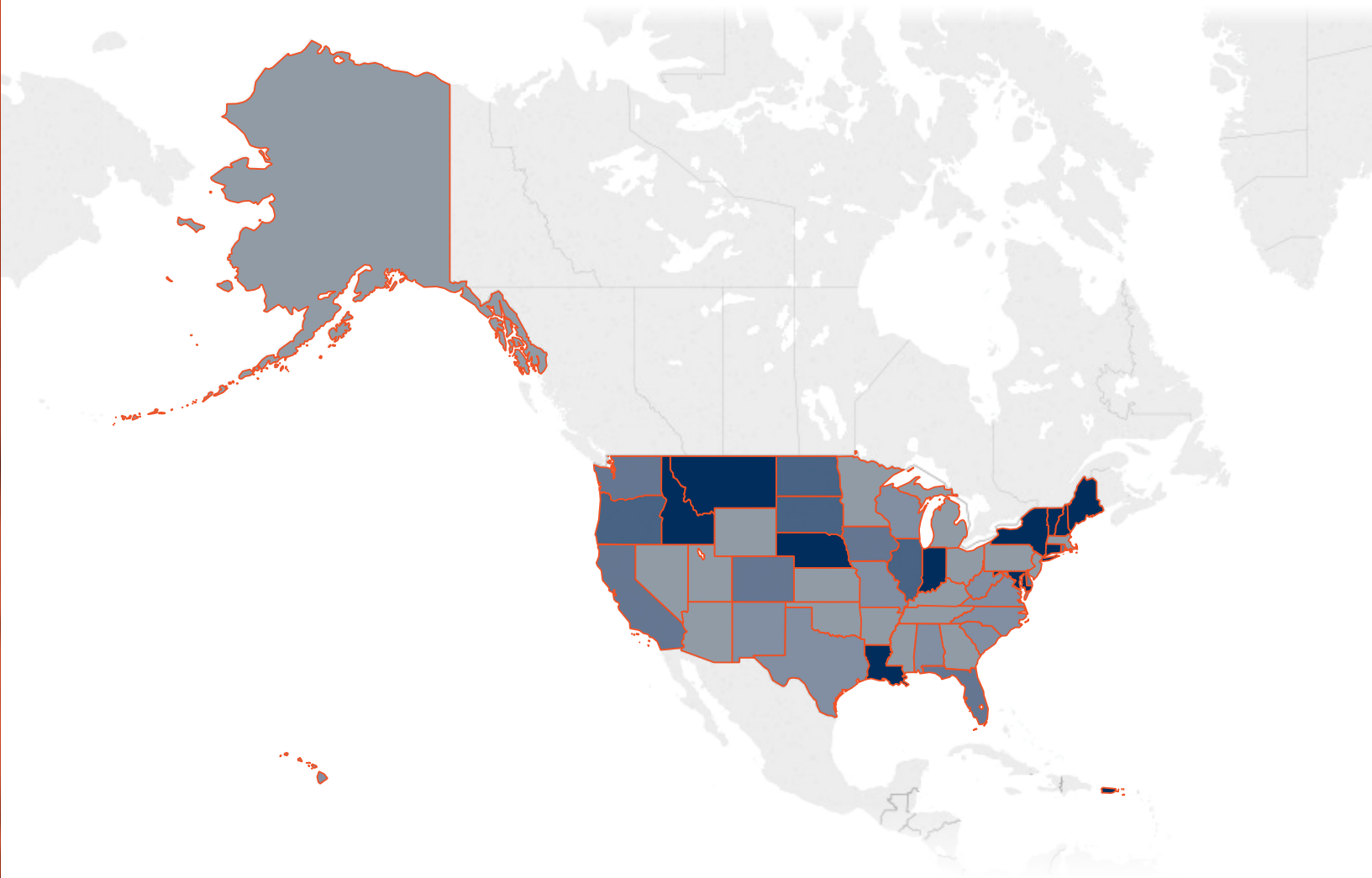
D

No explicit deadline in statute.

F

Grading State and Territory Notification Requirements

Alabama	Florida	Kentucky	Montana	Ohio	Texas
Alaska	Georgia	Louisiana	Nebraska	Oklahoma	U.S. Virgin Islands
Arizona	Guam	Maine	Nevada	Oregon	Utah
Arkansas	Hawaii	Maryland	New Hampshire	Pennsylvania	Vermont
California	Idaho	Massachusetts	New Jersey	Puerto Rico	Virginia
Colorado	Illinois	Michigan	New Mexico	Rhode Island	Washington
Connecticut	Indiana	Minnesota	New York	South Carolina	West Virginia
Delaware	Iowa	Mississippi	North Carolina	South Dakota	Wisconsin
District of Columbia	Kansas	Missouri	North Dakota	Tennessee	Wyoming



Requires notice to Attorney General
when any resident is affected.

A

Requires notice to Attorney General
when 250 residents are affected.

B

Requires notice to
Attorney General when
500 residents are affected.

C

Requires notice to Attorney
General when 1,000 to
10,000 residents are affected.

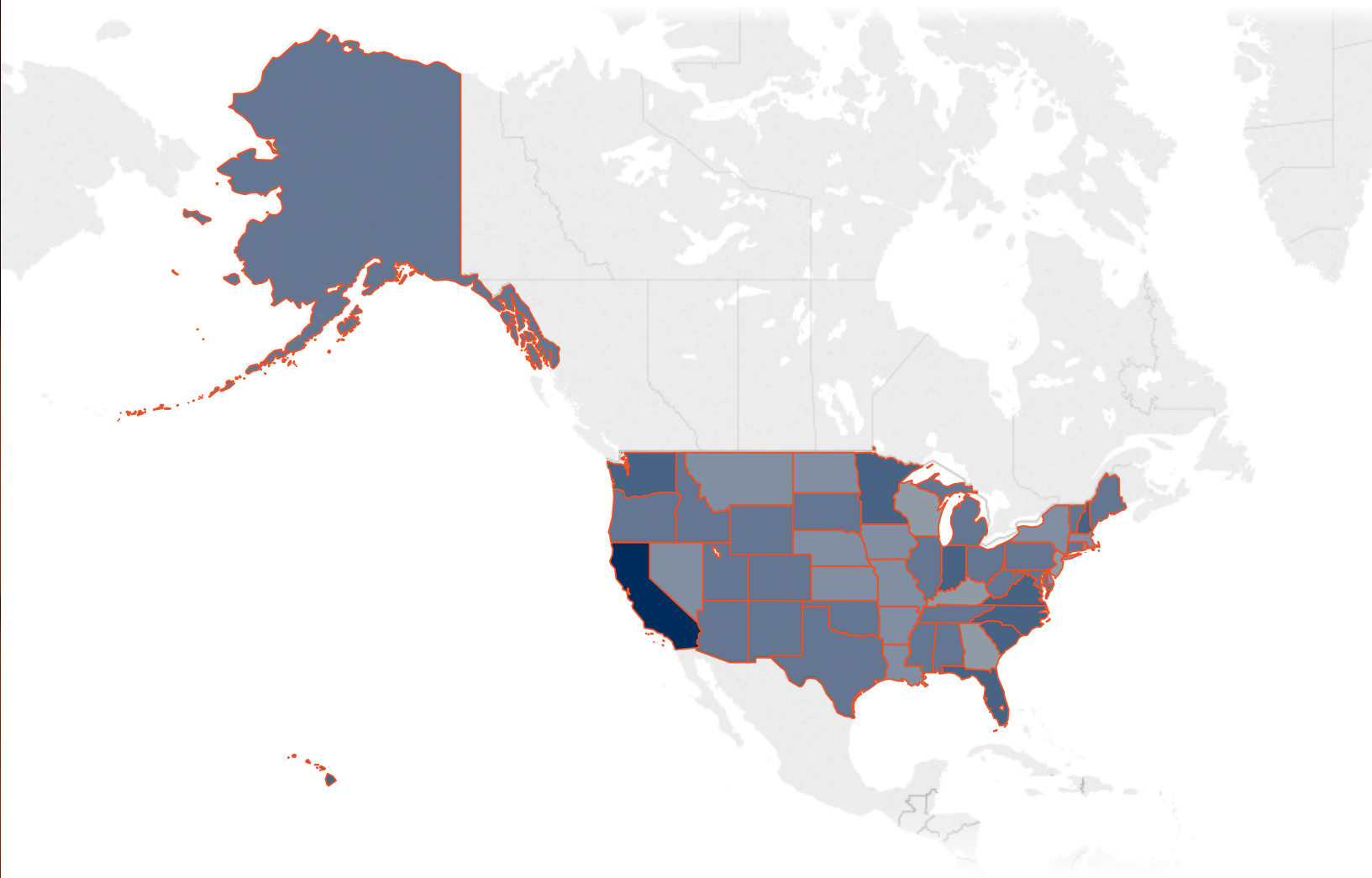
D

Does not require notice
to the Attorney General.

F

Grading State and Territory Enforcement Measures for Violations

Alabama	Florida	Kentucky	Montana	Ohio	Texas
Alaska	Georgia	Louisiana	Nebraska	Oklahoma	U.S. Virgin Islands
Arizona	Guam	Maine	Nevada	Oregon	Utah
Arkansas	Hawaii	Maryland	New Hampshire	Pennsylvania	Vermont
California	Idaho	Massachusetts	New Jersey	Puerto Rico	Virginia
Colorado	Illinois	Michigan	New Mexico	Rhode Island	Washington
Connecticut	Indiana	Minnesota	New York	South Carolina	West Virginia
Delaware	Iowa	Mississippi	North Carolina	South Dakota	Wisconsin
District of Columbia	Kansas	Missouri	North Dakota	Tennessee	Wyoming



The state statute contains three key elements: (1) PRA; (2) Has a high cap on damages (500/750k); (3) Violation constitutes an Unfair and Deceptive Practice.

A

The state statute contains at least two elements: (1) PRA and (2) Either a low cap on damages, or a violation constitutes an Unfair and Deceptive Practice.

B

The state statute provides either: (1) a low cap on damages or (2) violation of the act constitutes an Unfair and Deceptive Practice.

C

The state statute provides (1) a low cap on damages; or (2) the AG can only sue for an injunction.

D

No applicable provision.

F



**Massive
Amounts of
Data Records
Breach**

**Our
Country**



No comprehensive
Right to **Privacy**



Little Trust
in those who **collect, use**
and **share** our data



Lack of **Power**
to protect our privacy

Protecting Privacy for All



Since 1992, Privacy Rights Clearinghouse has been **protecting privacy for all** by **empowering individuals** and **advocating for positive change**.

We focus exclusively on consumer privacy rights and issues, and strive to provide clarity on complex topics by **publishing extensive educational materials** and directly **answering people's questions**. We are also **amplifying the public's voice** through their individual stories—often underrepresented in policy discussions—in our work **championing strong privacy protections**.

We hope that this report has been useful. If you would like to support the development and creation of further educational materials, please consider donating to our organization.

**Our
Mission**

privacyrights.org/donate



Privacy Rights Clearinghouse

3033 5th Avenue
Suite 223
San Diego, CA 92103

O: (619) 298-3396
F: (619) 255-4719

privacyrights.org