BakerHostetler

Data Breach Charts

November 2017

BakerHostetler

DATA BREACH CHARTS

The following standard definitions of Personal Information and Breach of Security (based on the definition commonly used by most states) are used for ease of reference, and any variations from the common definition are noted:

Personal Information: An individual's first name or first initial and last name plus one or more of the following data elements: (i) Social Security number, (ii) driver's license number or state-issued ID card number, (iii) account number, credit card number or debit card number combined with any security code, access code, PIN or password needed to access an account and generally applies to computerized data that includes personal information. Personal Information shall not include publicly available information that is lawfully made available to the general public from federal, state or local government records, or widely distributed media. In addition, Personal Information shall not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Breach of Security: The unlawful and unauthorized acquisition of personal information that compromises the security, confidentiality, or integrity of personal information.

Please note that the following summary of state data breach statutes are not intended to be and should not be used as a substitute for reviewing the statutory language, nor do they constitute legal advice. If you find these charts helpful and require legal counsel, please contact BakerHostetler's Privacy and Data Protection Team. Our blog is: www.dataprivacymonitor.com.

States in Which Definition for "Personal Information" is Broader than the General Definition	
Alaska	**Personal Information** of Alaska residents. In addition: passwords, personal identification numbers, or other access codes for financial accounts.
Arkansas	**Personal Information** of Arkansas residents. In addition: medical information.
California	General Breach Notification Statute: **Personal Information** of California residents. In addition: a username or email address, in combination with a password or security question and answer that would permit access to an online account; information or data collected through the use or operation of an automated license plate recognition system; medical information and health insurance information. Medical Information Specific Breach Notification Statute: For clinics, health facilities, home health agencies, and hospices licensed pursuant to sections 1204, 1250, 1725, or 1745 of the California Health and Safety Code, the state's Medical Information Breach Notification statute may apply. The statute applies to patients' medical information. "Medical information" means any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment. "Individually identifiable" means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, electronic mail address, telephone number, or Social Security number, or other information that, alone or in combination with other publicly available information, reveals the individual's identity.
Connecticut	**Personal Information** of Connecticut residents. In addition: (1) protected health information; (2) taxpayer identification numbers; (3) alien registration numbers; (4) government passport numbers; (5) demand deposit account numbers; (6) savings account numbers; (7) credit card numbers; (8) debit card numbers; and (9) unique biometric data, such as a fingerprint, a voice print, a retina or an iris image, or other unique physical representations and biometric information. (Effective October 1, 2015).
Delaware	**Personal Information** of Delaware residents. Beginning April 14, 2018, personal information will also include an individual's first and last name or last name and first initial and any one or more of the following data elements: (1) a passport number; (2) a username or email address in combination with a password or security question and answer that would permit access to an online account; (3) medical history, mental or physical condition, medical treatment or diagnosis by a health care professional or deoxyribonucleic acid (DNA) profile; (4) health insurance policy number, subscriber identification number, or any unique identifier used by a health insurer to identify the person; (5) unique biometric data generated from measurements or analysis of human body characteristics for authentication purposes; (6) an individual taxpayer identification number.
Florida	**Personal Information** means either of the following:

States in Which Definition for "Personal Information" is Broader than the General Definition	
	a. An individual's first name or first initial and last name in combination with any one or more of the following data elements for that individual: (i) a social security number; (ii) a driver license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity; (iii) a financial account number or credit or debit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual's financial account; (iv) any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or (v) an individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual. b. A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account.
Georgia	**Personal Information** of Georgia residents. In addition: a password and any of the data elements not in connection with the name if any of the other data elements alone would be sufficient to perform or attempt to perform identity theft against the person whose information was compromised.
Iowa	**Personal Information** of Iowa residents. In addition: a unique electronic identifier or routing code, in combination with any required security code, access code, or password that would permit access to an individual's financial account; unique biometric data, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data.
Illinois	**Personal Information** of Illinois residents. Beginning January 1, 2017, "Personal Information" will also include medical information; health insurance information; unique biometric data generated from measurements of human body characteristics used to authenticate an individual, such as a fingerprint; and user name or email address, in combination with a password or security question and answer that would permit access to an online account.
Kansas	**Personal Information** of Kansas residents. In addition: an account number or credit card/debit card number, alone or in combination with any required security code, access code or password that would permit access to a consumer's financial account.
Maine	**Personal Information** of Maine residents. In addition: Account passwords or personal identification numbers or other access codes; or any single data element from the definition of PI when not in connection with the individual's first name, or first initial, and last name, if the information if compromised would be sufficient to permit a person to fraudulently assume or attempt to assume the identity of the person whose information was compromised.
Maryland	**Personal Information** of Maryland residents. In addition: an individual Taxpayer Identification Number.
Massachusetts	**Personal Information** of Massachusetts residents. In addition: financial account information with or without password or security code information. This includes non-electronic personal information.

States in Which Definition for "Personal Information" is Broader than the General Definition	
Missouri	**Personal Information** of Missouri residents. In addition: a unique electronic identifier or routing code in combination with required security code, access code, or password that would permit access to an individual's financial account; medical and health insurance information, including an individual's medical history, mental or physical condition, treatment or diagnosis, health insurance policy number and any other unique identifier used by a health insurer.
Montana	**Personal Information** of Montana residents. In addition: (1) medical record information as relates to an individual's physical or mental condition, medical history, medical claims history, or medical treatment; and is obtained from a medical professional or medical care institution, from the individual, or from the individual's spouse, parent, or legal guardian; (2) taxpayer identification number; or (3) an identity protection personal identification number issued by the United States internal revenue service. (Numbers 1 – 3 effective October 1, 2015).
Nebraska	**Personal Information** of Nebraska residents. In addition: a unique electronic identification number or routing code, in combination with any required security code, access code, or password; or unique biometric data, such as finger print, voice print, or retina or iris image, or other unique physical representation. A separate category of personal information is a user name or email address, in combination with a password or security question or answer, that would permit access to an online account (effective July 20, 2016).
Nevada	**Personal Information** of Nevada residents. In addition: (1) driver authorization card number or identification card number; (2) a medical identification number or a health insurance identification number; and (3) 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. (Numbers 1 through 3 effective July 1, 2016).
New Hampshire	Medical Information Unauthorized Disclosure Notification Statute: For persons, corporations, facilities, or institutions either licensed in New Hampshire or otherwise lawfully providing health care services, the state's Medical Information Unauthorized Disclosure Notification statute may apply. The statute applies to protected medical information from §§262 and 264 of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (codified at 42 U.S.C. § 300gg and 29 U.S.C § 1181 et seq. and 42 USC 1320d et seq. (2010)). Student Data Unauthorized Disclosure Notification Statute: "Student personally-identifiable data" means: (1) the student's name; (2) the name of the student's parents or other family members; (3) the address of the student or student's family; (4) indirect identifiers, including the student's date of birth, place of birth, social security number, email, social media address, or other electronic address, telephone number, credit card account number, insurance account number, and financial services account number; and (5) other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty. "Teacher personally-identifiable data" applies to teachers, paraprofessionals, principals, school employees, contractors, and administrators and means: (1) Social Security number; (2) date of birth; (3) personal street address; (4) personal email address; (5)

States in Which Definition for "Personal Information" is Broader than the General Definition	
	personal telephone number; (6) performance evaluations; and (7) other information that, alone or in combination, is linked or linkable to a specific teacher, paraprofessional, principal, or administrator that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify any with reasonable certainty. .
New Jersey	**Personal Information** of New Jersey residents. In addition: dissociated data that, if linked, would constitute personal information is personal information if the means to link the dissociated data were accessed in connection with access to the dissociated data.
New Mexico	**Personal Information** of New Mexico residents. In addition: biometric data, such as an individual's fingerprints, voice print, iris or retina patterns, facial characteristics or hand geometry that is used to uniquely and durably authenticate an individual's identity.
New York	The law applies to "private information," which means personal information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person, in combination with any one or more of the following data elements: (1) Social Security number; (2) driver's license number or non-driver identification 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 an individual's financial account. The law statute covers "private information," which is personal information consisting of any information in combination with any one or more of the following data elements: (1) social security number; (2) driver's license number or non-driver identification 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 an individual's financial account. "Personal information" means any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person. Private information does not include publicly available information which is lawfully made available to the general public from federal, state, or local government records.
North Carolina	A person's first name or initial and last name, in combination with any one or more of the following: (1) Social Security number; (2) driver's license or State ID number; (3) account number, credit or debit card number, in combination with security or access codes or passwords to an individual's financial account; (4) digital signature; (5) biometric data; (6) finger prints; (7) other information that would permit access to a person's financial account or resources. Personal Information does not include electronic identification numbers, electronic mail names or addresses, Internet account numbers, Internet

States in Which Definition for "Personal Information" is Broader than the General Definition	
	identification names, parents' legal surname prior to marriage, or a password unless this information would permit access to a person's financial account or resources.
North Dakota	"Personal information" means an individual's first name or first initial and last name in combination with any of the following data elements, when the name and the data elements are not encrypted: (1) the individual's social security number; (2) the operator's license number assigned to an individual by the department of transportation; (3) a nondriver color photo identification card number assigned to the individual by the department of transportation; (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. (Underlined portion of number 9 effective August 1, 2015).
Ohio	**Personal Information** of Ohio residents, excluding publicly available information that is lawfully available to the general public from federal, state, or local government records or any of the following media that are widely distributed: 1) any news or editorial advertising statement published in any bona fide newspaper, journal, or magazine, or broadcast over radio or television; 2) any gathering or furnishing of information or news by any bona fide reporter, correspondent, or news bureau to news media; 3) any publication designed for and distributed to members of any bona fide associations or charitable or fraternal nonprofit corporation; 4) any type of media similar in nature to any item, entity, or activity identified above.
Oregon	A consumer's first name or first initial and last name in combination with any one or more of the following data elements when the data elements are not rendered unusable through encryption, redaction or other methods, or when the data elements are encrypted and the encryption key has also been acquired: (1) Social Security number; driver license number or state identification card number issued by the Department of Transportation; (2) passport number or other United States issued identification number; or (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 a consumer's financial account. (4) Biometric information used for authentication purposes (i.e., data from automatic measurements of a consumer's physical characteristics, such as an image of a fingerprint, retina or iris, that are used to authenticate the

States in Which Definition for "Personal Information" is Broader than the General Definition	
	consumer's identity in the course of a financial transaction or other transaction). (5) A consumer's health insurance policy number or health insurance subscriber identification number (if in combination with any other unique identifier that a health insurer uses to identify the consumer). (6) Any information about a consumer's medical history or mental or physical condition or about a health care professional's medical diagnosis or treatment of the consumer. (Numbers 4-6 effective January 1, 2016). Personal information also includes any of the data elements or any combination of the data elements described above when not combined with the consumer's first name or first initial and last name and when the data elements are not rendered unusable through encryption, redaction or other methods, if the information obtained would be sufficient to permit a person to commit identity theft against the consumer whose information was compromised. Personal information DOES NOT include information, other than a Social Security number, in a federal, state or local government record that is lawfully made available to the public.
Rhode Island	Personal Information means an individual's first or name or first initial and last name combined with any one or more of the following, if not encrypted or in hard copy paper format: (1) Social Security number; (2) Driver's license number or Rhode Island identification card number or tribal identification card number; (3) Account number, credit or debit card number, in combination with any required security code, access code, password or personal identification number that would permit access to an individual's financial account; (4) Medical or health insurance information; or (5) Email address in combination with any required security code, access code, or password that would allow access to an individual's personal, medical, Insurance, or financial account. (Effective July 2, 2016).
South Carolina	**Personal Information** of South Carolina residents. In addition: other numbers or information which may be used to access a person's financial accounts or numbers or information issued by a governmental or regulatory entity that uniquely will identify an individual.
Texas	The statute applies to "Sensitive personal information", which includes **Personal Information** of Texas residents. In addition: information that identifies an individual and relates to: 1) the physical or mental health or condition of the individual; 2) the provision of health care to the individual; or 3) payment for the provision of health care to the individual.
Vermont	"Personally identifiable information" of Vermont residents, which means an individual's first name or first initial and last name in combination with any one

States in Which Definition for "Personal Information" is Broader than the General Definition	
	or more of the following data elements when either the name or the data elements are not encrypted, redacted, or otherwise protected: (i) Social Security number; (ii) motor vehicle operator's license number or non-driver identification card number; (iii) financial account number or credit or debit card number, if circumstances exist in which the number could be used without additional identifying information, access codes, or passwords; (iv) account passwords or personal identification numbers or other access codes for a financial account.
Virginia	Personal Information Breach Notification Statute: **Personal Information** of Virginia residents. In addition: medical information. Medical Information Breach Notification Statute: For an authority, board, bureau, commission, district or agency of the state or of any political subdivision of the state, or agencies in the state supported wholly or principally by public funds, the state's Medical Information Breach Notification statute may apply. The statute applies to Medical information. "Medical information" means the first name or first initial and last name with any of the following elements: (1) any information regarding an individual's medical or mental health history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or (2) an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.
Wisconsin	An individual's last name and the individual's first name or first initial, in combination with and linked to any of the following elements, if the element is not publicly available information and is not encrypted, redacted, or altered in a manner that renders the element unreadable: (1) the individual's Social Security number; (2) the individual's driver's license number or state identification number; (3) the number of the individual's financial account number, including a credit or debit card account number, or any security code, access code, or password that would permit access to the individual's financial account; (4) DNA profile; (5) the individual's unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation.
Wyoming	"Personal identifying information", which includes the first name or first initial and last name of a person in combination with one or more of the following data elements when either the name or the data elements are not redacted: (A) Social Security number; (B) driver's license number or Wyoming identification card number; (C) account number, credit card number or debit card number in combination with any security code, access code or password that would allow access to a financial account of the person; (D) tribal identification card; or (E) federal or state government issued identification card. (F) username or email address, in combination with a password or security question and answer that would permit access to an online account;

States in Which Definition for "Personal Information" is Broader than the General Definition	
	(G) birth or marriage certificate; (H) medical information, meaning a person's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; (I) 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; (J) unique biometric data, meaning data generated from measurements or analysis of human body characteristics for authentication purposes; or (K) individual taxpayer identification number.
District of Columbia	A person's first name or first initial and last name, or phone number, or address, in combination with one of the following: (1) Social Security number; (2) driver's license number or District of Columbia Identification Card number (3) credit card number or debit card number; or any other number or code or combination of numbers or codes, such as account number, security code, access code, or password, that allows access to or use of an individual's financial or credit account.
Puerto Rico	At least the name or first initial and the surname of a person, together with any of the following data so that an association may be established between certain information with another and in which the information is legible enough so that in order to access it there is no need to use a special cryptographic code: (1) Social Security number; (2) driver's license number, voter's identification or other official identification; (3) bank or financial account numbers of any type with or without passwords or access code that may have been assigned; (4) names of users and passwords or access codes to public or private information systems; (5) medical information protected by the HIPAA; (6) tax information; (7) work-related evaluations.

States that Trigger Notification by Access	
Connecticut	"Breach of security" means unauthorized access to or unauthorized acquisition of electronic files, media, databases, or computerized data containing personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable.
New Jersey	"Breach of security" means unauthorized access to electronic files, media or data containing personal information that compromises the security, confidentiality or integrity of personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable.
Puerto Rico	"Violation of the system's security" means any situation in which it is detected that access has been permitted to unauthorized persons or entities to the data files so that the security, confidentiality or integrity of the information in the data bank has been compromised; or when normally authorized persons or entities have had access and it is known or there is reasonable suspicion that they have violated the professional confidentiality or obtained authorization under false representation with the intention of making illegal use of the information. This includes both access to the data banks through the system and physical access to the recording media that contain the same and any removal or undue retrieval of said recordings.

States That Require a Risk of Harm Analysis in Determining When Notification is Triggered	
Alaska	Notice is not required if, after an investigation and written notice to the Attorney General, the entity determines that there is not a reasonable likelihood that harm to the consumers has or will result. The determination must be documented in writing and maintained for five years.
Arizona	Notice is not required if the breach does not materially compromise the security of the personal information maintained or if the entity or a law enforcement agency, after a reasonable investigation, determines that a breach of the security of the system has not occurred or is not reasonably likely to occur.
Arkansas	Notification under this section is not required if, after a reasonable investigation, the person or business determines that there is no reasonable likelihood of harm to customers.
Colorado	Notification is not required if after a good-faith, prompt and reasonable investigation, the entity determines that misuse of personal information about a Colorado resident has not occurred and is not likely to occur.
Connecticut	Notification is not required if, after a reasonable investigation and consultation with relevant law enforcement agencies, it is determined that there is no reasonable likelihood of harm to customers.
Delaware	Notification is only required if an investigation determines that the 32 use of information about a Delaware resident has occurred or is reasonably likely to occur. Effective April 14, 2018, notification is required unless, after an appropriate investigation, the person reasonably determines that the breach of security is unlikely to result in harm to the individual whose personal information has been breached.
Florida	Notice to the affected individuals is not required if, after an appropriate investigation and consultation with relevant federal, state, or local 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 documented in writing and maintained for at least 5 years.
Hawaii	Notification is not required if the entity determines after a reasonable investigation that there is no reasonable likelihood of harm.
Idaho	Notification required if the security, confidentiality, or integrity of the personal information for one or more persons is materially compromised and an investigation determines that the misuse of information about an Idaho resident has occurred or is reasonably likely to occur.
Indiana	Notification required if the database owner knows, should know, or should have known that the unauthorized acquisition constituting the breach has resulted in or could result in identity deception, identity theft, or fraud affecting the Indiana resident.
Iowa	Notification is not required if, after an appropriate investigation or after consultation with the relevant federal, state, or local agencies responsible for law enforcement, the person determined that no reasonable likelihood of financial harm to the consumers whose personal information has been acquired has

States That Require a Risk of Harm Analysis in Determining When Notification is Triggered	
	resulted or will result from the breach. Such a determination must be documented in writing and the documentation must be maintained for five years.
Kansas	Any entity to which the statute applies shall, when it becomes aware of any breach of the security of the system, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused. If the investigation determines that the misuse of information has occurred or is reasonably likely to occur, the person or government, governmental subdivision or agency shall give notice as soon as possible to the affected Kansas resident.
Kentucky	Notification is required if the unauthorized acquisition of unencrypted and unredacted computerized data that compromises the security, confidentiality, or integrity of personally identifiable information maintained by the information holder as part of a database regarding multiple individuals actually causes or leads the information holder to reasonably believe has caused or will cause identity theft or fraud against any Kentucky resident.
Louisiana	Notification is not required if after reasonable investigation the person or business determines that there is no reasonable likelihood of harm to customers.
Maine	Notification is not required if after conducting a good-faith, reasonable and prompt investigation, the entity determines that there is not a reasonable likelihood that the personal information has been or will be misused.
Maryland	Notification is not required if after a good-faith, reasonable and prompt investigation the entity determines that the personal information of the individual was not and will not be misused as a result of the breach. If after the investigation is concluded, the entity determines that notification is not required, the entity shall maintain records that reflect its determination for three years after the determination is made.
Massachusetts	The breach must create a substantial risk of identity theft or fraud against a resident of the commonwealth or when the person or agency knows or has reason to know that the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose.
Michigan	The person or agency does not have to provide notice if the person or agency determines that the security breach has not or is not likely to cause substantial loss or injury to, or result in identity theft with respect to, one or more residents of Michigan. In making this determination, a person or agency shall act with the care an ordinarily prudent person or agency in like position would exercise under similar circumstances.
Mississippi	Notification is not required if, after an appropriate investigation, the person reasonably determines that the breach will not likely result in harm to the affected individuals.
Missouri	Notification is not required if, after an appropriate investigation by the person or after consultation with the relevant federal, state, or local agencies responsible for law enforcement, the person determines that a risk of identity theft or other fraud to any consumer is not reasonably likely to occur as a result of the breach. Such a determination shall be documented in writing and the documentation shall be maintained for five years.
Montana	Notification required if the unauthorized acquisition of computerized data materially compromises the security, confidentiality, or integrity of personal

States That Require a Risk of Harm Analysis in Determining When Notification is Triggered	
	information and causes or is reasonably believed to cause loss or injury to a Montana resident.
Nebraska	If the investigation determines that the use of information about a Nebraska resident for an unauthorized purpose has occurred or is reasonably likely to occur, the individual or commercial entity shall give notice to the affected Nebraska resident.
Nevada	Notification is required if the unauthorized acquisition of computerized data materially compromises the security, confidentiality, or integrity of personal information maintained by the data collector.
New Hampshire	For Personal Information Breach Notification Statute: Notification is not required if it is determined that misuse of the information has not occurred and is not reasonably likely to occur.
New Jersey	Notification is not required if the business or public entity establishes that misuse of the information is not reasonably possible (must retain a record of this decision for five years).
New Mexico	Notification is not required if, after an appropriate investigation, the person determines that the security breach does not give rise to a significant risk of identity theft or fraud.
New York	In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization, such business may consider the following factors, among others: (1) indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information; or (2) indications that the information has been downloaded or copied; or (3) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.
North Carolina	Notification not required if a breach does not result in illegal use of personal information, is not reasonably likely to result in illegal use, or there is no material risk of harm to a consumer.
Ohio	Notification required only if the access and acquisition by the unauthorized person causes or reasonably is believed will cause a material risk of identity theft or other fraud to the resident.
Oklahoma	Notification required if the breach causes, or the individual or entity reasonably believes has caused or will cause, identity theft or other fraud to any resident of this state.
Oregon	For a person that owns the data, notification is not required if, after an appropriate investigation or after consultation with relevant federal, state or local agencies responsible for law enforcement, 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. Such a determination must be documented in writing and the documentation must be maintained for five years.
Pennsylvania	Notification required only if the access and acquisition materially compromises the security or confidentiality of personal information.

States That Require a Risk of Harm Analysis in Determining When Notification is Triggered	
South Carolina	Notification required when personal identifying information that was not rendered unusable through encryption, redaction, or other methods was, or is reasonably believed to have been, acquired by an unauthorized person, and the illegal use of the information has occurred or is reasonably likely to occur or use of the information creates a material risk of harm to the resident.
Tennessee	Notification required for unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the information holder.
Utah	Notification required if misuse of personal information for identity theft or fraud purposes has occurred, or is reasonably likely to occur
Vermont	Notice of a security breach is not required if the data collector establishes that misuse of personal information is not reasonably possible and the data collector provides notice of the determination and a detailed explanation for said determination to the Vermont attorney general or to the department of banking, insurance, securities, and health care administration. If the data collector later gathers facts to indicate that the misuse of personal information is reasonably possible, then notice is required.
Virginia	Notification required if the entity reasonably believes that such a breach has caused or will cause identity theft or other fraud to any resident of the Commonwealth.
Washington	A person, business, or agency shall not be required to disclose a technical breach of the security system that does not seem reasonably likely to subject customers to a risk of harm.
West Virginia	Notification required only if the individual or entity reasonably believes the breach has caused or will cause identity theft or other fraud to any resident of this State.
Wisconsin	Notification is not required if the acquisition of personal information does not create a material risk of identity theft or fraud to the subject of the personal information.
Wyoming	Notification is required when unauthorized acquisition of computerized data 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. Residents must be notified of a breach of the security of the system when, after a good faith, reasonable, and prompt investigation, the individual or commercial entity determines that the misuse of personal identifying information about the residents has occurred or is reasonably likely to occur.

States that Require Notice to Attorney General or State Agency	
Alaska	If an entity determines after an investigation that the breach does not create a reasonable likelihood that harm to the consumers has or will result, it must document this determination and provide notice of the determination to the Attorney General.
California	General Breach Notification Statute: Any person who notifies more than 500 California residents as a result of a single breach must complete and submit the Attorney General's Data Security Breach form, and attach a single sample copy of the notification letter sent to affected California residents. Medical Information Specific Breach Notification Statute: The California Department of Health Services must be notified no later than 5 business days (15 business days effective Jan. 1, 2015) after the unauthorized access, use, or disclosure has been detected by the licensee. Notice to the California Insurance Department: the Department requests that all insurers, insurance producers, and insurance support organizations provide the Insurance Commissioner any notices or information submitted to the Attorney General.
Connecticut	If notice of a breach of security is required to be provided to affected individuals, the person must also provide notice of the breach to the Attorney General not later than the time when notice is provided to residents. Pursuant to Bulletin IC-25 (Aug. 18, 2010), all licensees and registrants of the Connecticut Insurance Department are required to notify the Department of any information security incident which affects any Connecticut residents as soon as the incident is identified, but no later than five calendar days after the incident is identified.
Delaware	Beginning April 14, 2018, covered persons must provide notice to the Delaware Attorney General's Office of any breach of security requiring notice to more than 500 Delaware residents.
Florida	A covered entity shall provide notice to the Florida Attorney General's Office of any breach of security affecting 500 or more Florida residents. Such notice shall be provided as expeditiously as practicable, but no later than 30 days after determination of the breach or reason to believe a breach has occurred.
Hawaii	If the breach involves over 1000 persons, the Hawaii Office of Consumer Protection must be notified of the timing, content and distribution of the notice.
Idaho	If the entity is a public agency, it must notify the Attorney General within 24 hours of discovery. The agency must also report a security breach to the Office of the Chief Information Officer within the Department of Administration, pursuant to the Information Technology Resource Management Council policies.
Illinois	Beginning January 1, 2017, any state agency that suffers a single breach affecting the personal information of more than 250 Illinois residents must provide notice of the breach to the Illinois Attorney General within 45 days or at the same time the state agency provides notice to consumers (whichever is sooner). Notification to the Attorney General must include: (1) the types of personal information compromised in the breach; (2) the number of Illinois residents affected by the breach at the time of notification; (3) any steps the state agency

States that Require Notice to Attorney General or State Agency	
	has taken or plans to take relating to notification of the breach to consumers; and (4) the date and timeframe of the breach, if known at the time notification is provided. Any state agency that collects personal information and has had a breach of security of the system data or written material shall submit a report within five business days of the discovery or notification of the breach to the General Assembly listing the breaches and outlining any corrective measures that have been taken to prevent future breaches of the security of the system data or written material. Any agency that has submitted a report under the statute shall submit an annual report listing all breaches of security of the system data or written materials and the corrective measures that have been taken to prevent future breaches.
Indiana	The Attorney General must be notified regarding a breach.
Iowa	For a breach of security requiring notification of 500 or more Iowa residents pursuant to Iowa law, written notification must be provided to the director of the consumer protection division of the Iowa Attorney General within five business days of notifying any Iowa residents regarding the breach. (Effective July 1, 2014)
Louisiana	When notice must be given to Louisiana citizens, the entity must provide written notice detailing the breach of the security of the system to the Consumer Protection Section of the Attorney General's office. Notice shall include names of all Louisiana citizens affected. Notice to the state Attorney General shall be timely if received within 10 days of the distribution of notice to LA citizens. Each day notice is not received by the state Attorney General shall be deemed a separate violation.
Maine	The Attorney General or Department of Professional and Financial Regulation if the entity is governed by that body must be notified regarding a breach. Notice to the Maine Bureau of Insurance: Bulletin 345 provides that those licensed by the Superintendent – insurers, producers, adjusters, and third-party administrators – are required to notify the Superintendent of breaches that require notice under the Data Act, 10 M.R.S.A. §§ 1346-1349. The notice should include a description of the breach; the number of Maine residences affected; a copy of the notice and other information sent to affected persons; a description of the curative steps taken; and the name and contact information for the person whom the Superintendent may contact.
Maryland	The Attorney General must be notified prior to notification of individuals.
Massachusetts	The Attorney General, Director of Consumer Affairs and Business Regulation, must be notified regarding a breach. Upon receipt of notice, the Director of Consumer Affairs and Business Regulation will identify any relevant Consumer Reporting Agency or state agency that needs to be notified to the notifying party.
Missouri	If 1,000 or more persons are affected, then the Attorney General must be notified regarding the timing, distribution and content of notice to individuals.
Montana	Any person, business, or state agency required to make a notification must also simultaneously submit an electronic copy of the notification and a statement providing the date and method of distribution of the notification to the Montana Attorney General's Consumer Protection Office, excluding any information that personally identifies any individual who is entitled to receive notification. If

States that Require Notice to Attorney General or State Agency	
	notification is made to more than one individual, the notification must indicate the number of individuals in the state who received notification. (Effective October 1, 2015).
Nebraska	An individual or commercial entity required to provide notice of a breach of security of the system to a Nebraska resident(s) must also, not later than the time when notice is provided to the Nebraska resident(s), provide notice of the breach of security of the system to the Nebraska Attorney General's Office (effective July 20, 2016).
New Hampshire	A person engaged in trade or commerce shall notify the regulator which has primary regulatory authority over such trade or commerce. All other persons shall notify the Attorney General's office. Notice to the Attorney General's office must include the anticipated date of the notice to the individuals and the approximate number of individuals in the state who will be notified. The names of the individuals entitled to receive notice do not have to be disclosed. Student Data Unauthorized Disclosure Notification Statute: The New Hampshire Department of Education must submit an annual data security breach report to the governor, state board, senate president, speaker of the house of representatives, chairperson of the senate committee with primary jurisdiction over education, chairperson of the house committee with primary jurisdiction over education, legislative oversight committee, and commissioner of the department of information technology. The breach report shall also be posted to the department's public Internet website and shall not include any information that itself would pose a security threat to a database or data system. The report shall include: (1) The name of the organization reporting the breach. (2) Any types of personal information that were or are reasonably believed to have been the subject of a breach. (3) The date, estimated date, or date range of the breach. (4) A general description of the breach incident. (5) The estimated number of students and teachers affected by the breach, if any. (6) Information about what the reporting organization has done to protect individuals whose information has been breached. Notice to the New Hampshire Insurance Department: Any entity regulated by the New Hampshire Insurance Department is required to notify the department of any security breach.
New Jersey	The Division of State Police in the Law Department of Law and Public Safety must be notified regarding a breach prior to notifying customers.
New Mexico	For a breach of security requiring notification of more than 1,000 New Mexico residents, notification must be made to the office of the New Mexico Attorney General and the major consumer reporting agencies. Notification shall be made in the most expedient time possible, and no later than **forty-five (45) calendar days** subject to the determination by law enforcement that notification would impede a criminal investigation or as necessary to determine the scope of the incident and restore the integrity, security, and confidentiality of the data system.

States that Require Notice to Attorney General or State Agency	
	When notifying the New Mexico Attorney General, a person shall disclose the number of New Mexico residents that received a notification and shall provide a copy of the notification sent to affected residents.
New York	The Attorney General, Consumer Protection Board, and the state Office of Cyber Security and Critical Infrastructure must be notified regarding a breach via form notice.
North Carolina	The Consumer Protection Division of the Attorney General's Office must be notified of the nature of the breach, the number of consumers affected, steps taken to investigate the breach, steps taken to prevent a similar breach in the future, and information regarding the timing, distribution, and content of the notice via form notice.
North Dakota	Any person that experiences a breach of the security system must disclose to the North Dakota Attorney General by mail or email any breach of the security system which exceeds 250 individuals. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and to restore the integrity of the data system. (Effective August 1, 2015).
Ohio	Notice to the Ohio Department of Insurance: the Department issued a bulletin that requires all persons or entities holding a license or certificate of authority from the superintendent of insurance to notify the department within fifteen (15) days of discovering a "loss of control" of policyholder's personal information. The notice is required for incidents affecting more than 250 Ohio residents.
Oregon	The Oregon Attorney General must be notified regarding a breach, either in writing or electronically, if a breach affects 250 Oregon residents or more. Notice must also be made to consumer reporting agencies when the breach affects at least 1,000 Oregon residents and provide the notice any police report number assigned to the breach of security. (Effective January 1, 2016).
Puerto Rico	The Department of Consumer Affairs must be notified regarding a breach as expeditiously as possible (within a non-extendable 10 days after the violation of the system is detected, parties shall inform the Department of Consumer Affairs, which shall make a public announcement of the fact within 24 hours of receiving information).
Rhode Island	In the event that more than five hundred (500) Rhode Island residents are affected by a breach, the Rhode Island Attorney General and major credit reporting agencies must be notified as to the timing, content and distribution of the notices and the approximate number of affected Rhode Island residents. This notice should be made without delaying notice to affected Rhode Island residents. (Effective July 2, 2016). Notice to Rhode Island Department of Business Regulation: Rhode Island Insurance Regulation 107 requires licensees of the Department, which includes insurance companies and producers, to notify the department of a breach of the security of computerized unencrypted data that poses a significant risk of identity theft.
South Carolina	If 1,000 or more persons are affected, the Consumer Protection Division of the Department of Consumer Affairs must be notified regarding a breach.
Texas	Notice to Texas Department of Insurance: Pursuant to Commissioner's Bulletin # B-0022-16A, a domestic insurer or HMO should contact its assigned financial

States that Require Notice to Attorney General or State Agency	
	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.
Vermont	Once notice is made to consumers, the Attorney General must be notified of the number of Vermont consumers affected and provided a copy of the notice. A second copy of the consumer notification letter, with personally identifiable information that was subject to the breach redacted, can also be provided to the attorney general which will be used for any public disclosure of the breach. In the event a data collector provides notice to more than 1,000 consumers at one time pursuant to this section, the data collector shall notify, without unreasonable delay, all consumer reporting agencies. In notice to a consumer reporting agency, the data collector must include the timing, distribution, and content of the notices being sent to the affected consumers. Notice to Vermont Department of Banking, Insurance, Securities and Health Care Administration: the Department issued Bulletins, 1 and 3, providing that the state breach notification law applies to insurance companies, captive insurance companies, debt adjusters, and any other public or private corporation, limited liability company, or business regulated by the department. Any entity regulated by the department must provide notice to the department within 14 days of discovering any electronic data security breach that compromises a consumer's nonpublic personally identifiable information.
Virginia	Personal Information Breach Notification Statute: The Office of the Attorney General must be notified following discovery of a breach of personal information. In the event an individual or entity provides notice to more than 1,000 persons at one time, they must notify, without unreasonable delay, both the Office of the Attorney General and all consumer reporting agencies of the timing, distribution, and content of the notice sent to affected residents. Medical Information Breach Notification Statute: The Office of the Attorney General and the Commissioner of Health must be notified following discovery of a breach of medical information. The entity must notify both the subject of the medical information and any affected resident of the Commonwealth, if those are not the same person. In the event an entity provides notice to more than 1,000 persons at one time, they must notify, without unreasonable delay, the Office of the Attorney General and the Commissioner of Health of the timing, distribution, and content of the notice sent to affected individuals.
Washington	Notice to the Washington Attorney General: Any person or business that is required to issue notification under RCW 19.255.010 and 42.56.590 to more than 500 Washington residents as a result of a single breach must, no more than 45 days after the breach is discovered, electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Washington Attorney General. The person or business must also provide to the Washington Attorney General the number of Washington consumers affected by the breach, or an estimate if the exact number is not known. The Washington Attorney General may bring an action in the name of the state, or as parens patriae on behalf of persons residing in the state, to enforce the law.

States that Require Notice to Attorney General or State Agency	
	For actions brought by the Washington Attorney General, the Washington legislature finds that the practices covered by the data breach notification law are matters vitally affecting the public interest and a violation of the law is not reasonable in relation to the development and preservation of business and is an unfair or deceptive act in trade or commerce and an unfair method of competition for purposes of applying the consumer protection act. Notice to Office of the Insurance Commissioner: As adopted under notice filed as WSR 13-07-053, all licensees must notify the insurance commissioner within two business days of such licensee determining that notification regarding a security breach of personal health or private information under RCW 19.255.010 and 45 C.F.R. 164 is required to be made to consumers or customers. The notification to the insurance commissioner must be in writing and include the number of customers or consumers potentially affected and what actions are being taken (Effective July 24, 2015).
Wisconsin	Notice to Office of the Commissioner of Insurance: Wisconsin licensed insurers, gift annuities, warranty plans, motor clubs, and employee benefit plan administrators are requested to notify the office of any unauthorized access to personal information of Wisconsin residents as soon as practicable, but not later than 10 days after it becomes aware of such unauthorized access.

States that Require Notification within a Specific Time Frame (other than the general provision that notification must be given in the most expedient time and manner possible and without unreasonable delay, consistent with the legitimate needs of law enforcement).	
California	Medical Information Specific Breach Notification Statute: For clinics, health facilities, home health agencies, and hospices licensed pursuant to sections 1204, 1250, 1725, or 1745 of the California Health and Safety Code, the state's Medical Information Breach Notification statute may apply. The statute requires licensees to notify both affected patients and the California Department of Health Services no later than 5 business days (15 business days effective Jan. 1, 2015) after the unauthorized access, use, or disclosure has been detected by the licensee.
Connecticut	Pursuant to Bulletin IC-25 (Aug. 18, 2010), all licensees and registrants of the Connecticut Insurance Department are required to notify the Department of any information security incident which affects any Connecticut residents as soon as the incident is identified, but no later than **5 calendar days** after the incident is identified. Notice of a breach must be given to Connecticut residents no later than **90 days** after discovery of a breach. (Effective Oct. 1, 2015)
Delaware	Effective April 14, 2018, notice must be made without unreasonable delay but not later than 60 days after determination of the breach of security, subject to the following exceptions: 1. A shorter time is required under federal law, 2. A law enforcement agency requests that the notice be delayed based on their determination that notice will impede a criminal investigation, or 3. The covered person cannot through reasonable diligence identify certain Delaware residents whose personal information was breached within 60 days. Such person must provide notice as soon as practicable after the determination that the breach of security included the personal information of such residents.
Florida	Notice must be provided without unreasonable delay; no later than **30 days**; law enforcement can delay notification.
Maine	If, after the completion of an investigation, notification is required under this section, the notification required by this section may be delayed for no longer than 7 business days after a law enforcement agency determines that the notification will not compromise a criminal investigation.
New Mexico	Notification, to both the affected residents and the New Mexico Attorney General, shall be made in the most expedient time possible, but not later than **forty-five (45) calendar days** following the discovery of the security breach, subject to a determination by law enforcement that notification would impede a criminal investigation or the need to determine the scope of the security breach and restore the integrity, security, and confidentiality of the data system.
Ohio	Notice must be provided in the most expedient time possible but not later than **45 days** following its discovery or notification of the breach in the security of the system, subject to the legitimate needs of law enforcement activities.
Rhode Island	Notice of the security breach to a consumer must be made in the most expedient time possible but no later than **45 calendar days** after confirmation of the breach. (Effective July 2, 2016).

States that Require Notification within a Specific Time Frame (other than the general provision that notification must be given in the most expedient time and manner possible and without unreasonable delay, consistent with the legitimate needs of law enforcement).	
Tennessee	Notification must be provided immediately, but no later than 45 days from the discovery of the notification of the breach, unless a longer period of time is required due to the legitimate needs of law enforcement (effective July 1, 2016). Any information holder that maintains computerized data that includes personal information that the information holder does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately, but no later than 45 days from when the breach became known by the information holder, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person (effective July 1, 2016).
Vermont	Notice of the security breach to a consumer shall be made in the most expedient time possible and without unreasonable delay, but not later than **45 days** after discovery.
Washington	Notice to residents and to the Washington Attorney General must be made in the most expedient time possible and without unreasonable delay, no more than **45 calendar days** after the breach is discovered, unless at the request of law enforcement or any measures necessary to determine the scope of the breach and to restore the integrity of the data system. Breach notices to consumers must be written in plain language and include the name and contact information of the reporting person or business; a list of the types of personal information that were or are reasonably believed to have been the subject of a breach; and the toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed personal information.
Wisconsin	Notice shall be provided within a reasonable time, not to exceed **45 days** after the entity learns of the acquisition of personal information. A determination as to reasonableness shall include consideration of the number of notices that an entity must provide and the methods of communication available to the entity.

States That Permit a Private Cause of Action	
Alaska	A person injured by a breach may bring an action against a non-governmental agency under the Unfair or Deceptive Act or Practices, AS 45.50.471 – 45.50.561.
California	Any customer injured by a violation of the general breach notification statute may institute a civil action to recover damages. Any business that violates, proposes to violate, or has violated this title may be enjoined.
Louisiana	A civil action may be instituted to recover actual damages resulting from the failure to disclose in a timely manner to a person that there has been a breach of the security system resulting in the disclosure of a person's personal information.
Maryland	Consumers may bring actions under Title 13 of the Maryland Code, the Unfair and Deceptive Trade Practices Act.
Massachusetts	Massachusetts consumers may seek damages under Chapter 93A, which allows for certain instances of treble damages.
Nevada	A private right of action exists for the data collector. A data collector that provides the requisite notice may commence an action for damages against a person that unlawfully obtained or benefited from personal information obtained from records maintained by the data collector.
New Hampshire	Persons injured as a result of a violation may bring an action for damages and for such equitable relief as the court deems necessary and proper. A prevailing plaintiff shall be awarded the costs of the suit and reasonable attorney's fees. An aggrieved individual whose health records were wrongly disclosed may bring a civil action under RSA 332-I:4 or RSA 332-I:5 and, if successful, shall be awarded special or general damages of not less than $1,000 for each violation, and costs and reasonable legal fees.
North Carolina	Provides a private right of action only if individual is injured as a result of the violation. Damages set at a maximum of up to $5,000, per incident, and provides for treble damages within this range. Injunctive relief also available.
Oregon	Compensation can be ordered by the state upon a finding that enforcement of the rights of consumers by private civil action would be so burdensome or expensive as to be impractical.
South Carolina	A resident of SC who is injured by a violation of this section, in addition to and cumulative of all other rights and remedies available at law, may: institute a civil action to recover damages in case of a willful and knowing violation; institute a civil action to recover only actual damages resulting from a violation in case of a negligent violation; seek an injunction to enforce compliance; and recover attorney's fees and court costs, if successful.
Tennessee	A violation under the data breach notification statute may also be a violation of the Tennessee Consumer Protection Act, which could give rise to a private cause of action.

States That Permit a Private Cause of Action	
Texas	A violation under the data breach notification statute may also be a violation of the Texas Deceptive Trade Practices Act, which could give rise to a private cause of action.
Virginia	Though generally enforced by the Attorney General, nothing in the data breach notification statute will preclude recovery of economic damages.
Washington	Any customer injured by a violation may institute a civil action to recover damages.
District of Columbia	Any District of Columbia resident injured by a violation may institute a civil action to recover actual damages, the costs of the action, and reasonable attorney's fees. Actual damages shall not include dignitary damages, including pain and suffering.
Puerto Rico	Consumers may bring actions apart from the statute.
Virgin Islands	Any customer injured by a violation may commence a civil action to recover damages.

States With an Encryption Safe Harbor	
Alaska	The statute only applies to unencrypted information or encrypted information when the encryption key has also been disclosed.
Arizona	Notification requirement only applies where personal information was unencrypted.
Arkansas	Statute only applies to unencrypted data elements.
California	Notification under the general breach notification statute only applies where unencrypted personal information was acquired, or is believed to acquired, by an unauthorized person. As of January 1, 2017, California law will no longer include an encryption safe harbor. Beginning January 1, 2017, a notification obligation will be triggered where encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person together with the encryption key or security credential that "could render that personal information readable or useable."
Colorado	Statute applies only to the disclosure of unencrypted computerized data.
Connecticut	A breach of security only occurs when access to the personal information has not been secured by encryption or by any other method or technology that renders personal information unreadable or unusable.
Delaware	The statute applies to unencrypted computerized data. Effective April 14, 2018, the statute will apply to encrypted computerized data where the unauthorized acquisition includes, or is reasonably believed to include, the encryption key, and the person that owns or licenses the encrypted information has "a reasonable belief that the encryption key could render that personal information readable or useable."
Florida	The statute applies to unencrypted information.
Georgia	The statute applies to unencrypted personal information.
Hawaii	The statute applies only to disclosure of unencrypted or unredacted information.
Idaho	The statute applies to unencrypted personal information.
Illinois	The statute applies to not encrypted personal information.
Indiana	The statute does not apply to encrypted information, provided that the unauthorized recipient of the information does not also get an encryption key.
Iowa	The statute does not cover personal information if it is "encrypted, redacted, or otherwise altered in such a manner that the name or data elements are unreadable" unless the keys to unencrypt, unredact, or otherwise read the data have been obtained through a breach of security. (Effective July 1, 2014)
Kansas	The statute is triggered by disclosure of unencrypted or unredacted information.
Kentucky	The statute is triggered by unauthorized acquisition of unencrypted and unredacted computerized data.
Louisiana	Notification requirement only applies where the personal information was not encrypted or redacted.
Maine	The statute only applies to disclosure of information that is not encrypted.

States With an Encryption Safe Harbor	
Maryland	The statute only applies to disclosure of personal information that has not been encrypted, redacted, or otherwise protected by another method that renders the information unreadable or unusable.
Massachusetts	No notice is required as long as the data acquired or used is encrypted, and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information has not been acquired.
Michigan	A person or agency does not have to give notice if the resident's data was encrypted or redacted, and the person gaining unauthorized access did not have the encryption key.
Minnesota	A person or business must give notice of a security breach if personal information is acquired. Personal information does not include encrypted data.
Mississippi	Does not cover encrypted data.
Missouri	Personal information does not include information that is redacted, altered, or truncated such that no more than five digits of a social security number or the last four digits of a driver's license number, state identification card number, or account number is accessible as part of the personal information.
Montana	The statute applies only to disclosures of unencrypted information. Personal information is not considered to be encrypted if the encryption key or process is reasonably believed to have been acquired during the breach (effective July 20, 2016).
Nebraska	Notice is not required if data is encrypted or redacted.
Nevada	If the data is encrypted, notice is not required.
New Hampshire	If the data elements are encrypted, notification is not required.
New Jersey	Statute applies to personal information that has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable.
New Mexico	Notification is not required for encrypted or redacted personal identifying information or information that is otherwise rendered unreadable or unusable, unless the confidential process or key used to decrypt the data is compromised along with the encrypted data.
New York	When the private information is encrypted and the encryption key has not been acquired, there is no duty to notify.
North Carolina	Notification requirement only applies where the personal information acquired is unencrypted and unredacted.
North Dakota	Notification is not required when data has been secured by encryption or by any other method or technology that renders the electronic files, media, or data bases unreadable or unusable.
Ohio	If the data is encrypted, redacted, or altered by any method or technology in such a manner that the data elements are unreadable, notification is not required.
Oklahoma	Notification is not required for encrypted or redacted information unless the encrypted information is accessed and acquired in an unencrypted form or if the security breach involves a person with access to the encryption key and the

States With an Encryption Safe Harbor	
	individual or entity reasonably believes that such breach has caused or will cause identity theft or other fraud to any resident of this state.
Oregon	If data is encrypted or redacted, notice is not required. If the data is encrypted and the encryption key has also been required, notification is required.
Pennsylvania	Notification is not required when encrypted or redacted information is accessed and acquired. Notice is required, however, if encrypted information is accessed and acquired in an unencrypted form, if the security breach is linked to a breach of the security of the encryption or if the security breach involves a person with access to the encryption key.
Rhode Island	If the information is encrypted, notice is not required. "Encrypted" is defined as the transformation of data through the use of a 128 bit or higher algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key. (Encryption definition effective July 2, 2016).
South Carolina	If data is rendered unusable through encryption, redaction, or other methods, notice to consumers is not required.
Texas	"Sensitive personal information" only applies to data items that are not encrypted.
Utah	If the personal information is encrypted or protected by another method that renders the data unreadable or unusable, notice is not required.
Vermont	Data is not considered personal information if both the individual's name and the combined data element (i.e. social security number) are encrypted, redacted, or protected by another method that renders them unreadable or unusable.
Virginia	The unauthorized acquisition of encrypted or redacted data, without access to the encryption key, does not trigger the notice requirement under this statute.
Washington	The breach of secured personal information must be disclosed if the information acquired and accessed is not secured during a security breach or if the confidential process, encryption key, or other means to decipher the secured information was acquired by an unauthorized person (Effective July 24, 2015). If both an individual's first name or first initial and last name and accompanying data element (i.e. social security number) are "secured", notice is not required. "Secured" is defined as encrypted in a manner that meets or exceeds the National Institute of Standards and Technology (NIST) standard or is otherwise modified so that the personal information is rendered unreadable, unusable, or undecipherable by an unauthorized person. RCW 19.255.010 and 42.56.590. Also exempt are covered entities that are subject to the HIPAA/HITECH breach notification requirements or to the Interagency Guidance issued pursuant to the Gramm-Leach-Bliley Act.
West Virginia	If encrypted or redacted information is accessed and acquired and the person does not have access to the encryption key, notice is not required.
Wisconsin	If one of the data elements linked to an individual's name is encrypted, redacted, or altered in a manner that renders the element unreadable, it is not considered personal information, meaning no notice is required.

States With an Encryption Safe Harbor	
Wyoming	If both an individual's first name or first initial and last name and combined data element (i.e. social security number) are redacted, the data is not considered personal identifying information, and notice is not required.
District of Columbia	The acquisition of data that has been rendered secure, so as to be unusable by an unauthorized third party is not considered a breach of the security system.
Guam	Notification requirement does not apply to encrypted data unless the security breach involves a person with access to the encryption key and the individual or entity reasonably believes that such breach has caused or will cause identity theft or other fraud to any resident of Guam.
Puerto Rico	This statute is triggered only when unencrypted information is disclosed.
Virgin Islands	Statute applies only where personal information was unencrypted.

States Where the Statute is Triggered by a Breach of Security in Electronic and/or Paper Records	
Alaska	"Breach of security" means unauthorized acquisition, or reasonable belief of unauthorized acquisition, or personal information that compromises the security, confidentiality, or integrity of the personal information maintained by the information collector. "Acquisition" includes: acquisition by photocopying, facsimile, or other paper-based method; a device including a computer, that can read, write or store information that is represented in numerical form; or a method not identified by this paragraph.
Hawaii	This statute applies to any business that owns or licenses personal information of residents of Hawaii, any business that conducts business in Hawaii that owns or licenses personal information in any form (whether computerized, paper, or otherwise), or any government agency that collects personal information for specific government purposes.
Indiana	Breach of the security of data means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person. The term includes the unauthorized acquisition of computerized data that have been transferred to another medium, including paper, microfilm, or a similar medium, even if the transferred data are no longer in a computerized format.
Iowa	"Breach of security" means unauthorized acquisition of personal information maintained in computerized form by a person that compromises the security, confidentiality, or integrity of the personal information. "Breach of security" also means unauthorized acquisition of personal information maintained by a person in any medium, including on paper, that was transferred by the person to that medium from computerized form and that compromises the security, confidentiality, or integrity of the personal information. (Effective July 1, 2014)
Massachusetts	Breach of security is the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the commonwealth. Data is any material upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics.
North Carolina	Statute applies to any business that owns or licenses personal information in any form (whether computerized, paper or otherwise) or any business that maintains or possesses records or data containing personal information that the business does not own or license.
Washington	Any person, business, or agency that conducts business in Washington and that owns or licenses computerized any data (computerized or hard copy) that includes personal information of residents of Washington, and any person, business, or agency that maintains computerized data that includes personal information is subject to the data breach notification laws.
Wisconsin	This statute does not define a "breach of security", and its definition of "personal information" is not restricted to computerized information alone.