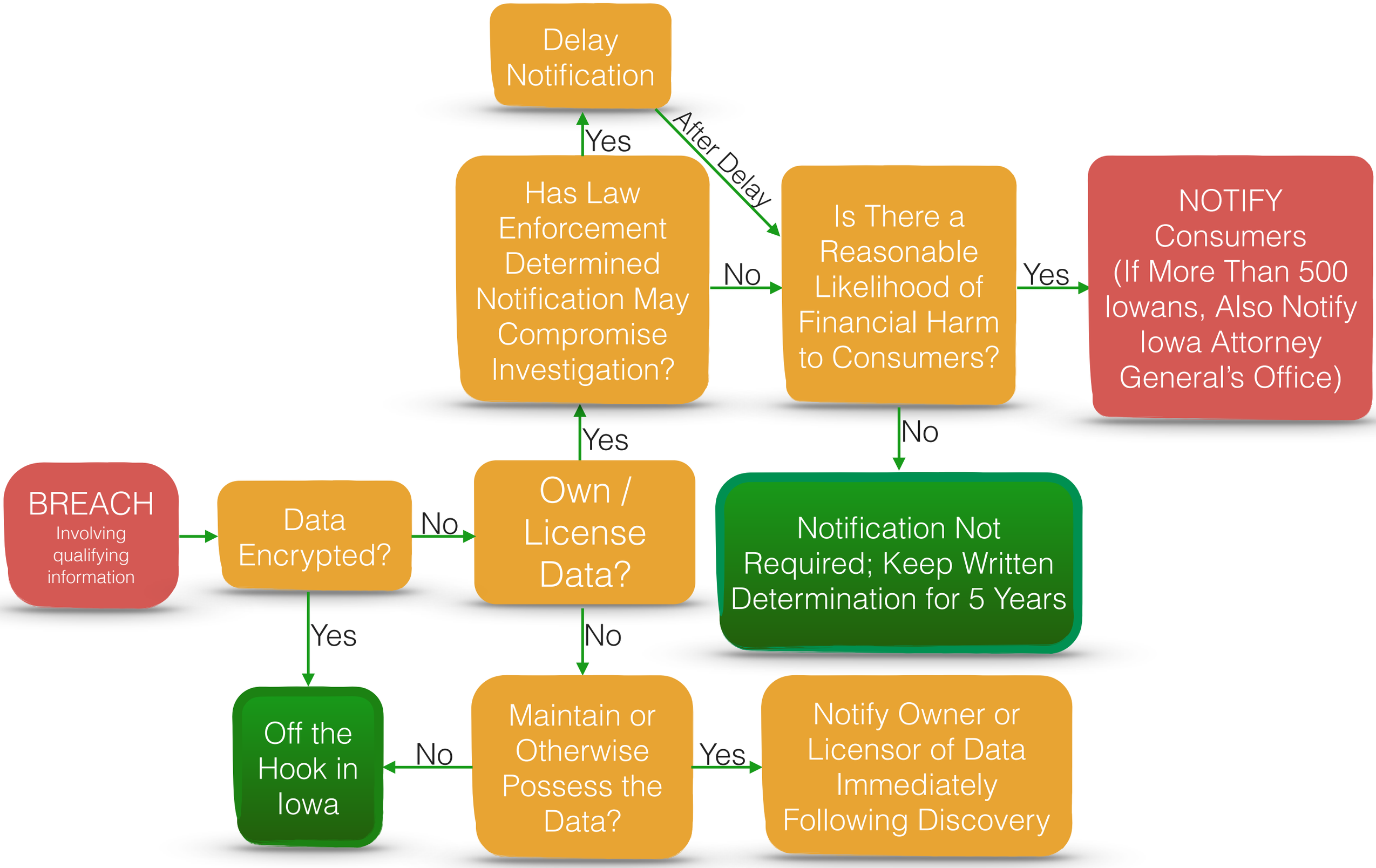
Data Breach Compliance Manual

Prepared by: BrownWinick Data Security & Privacy Practice Group

Date Prepared: July 2017

Iowa's Breach Notification Map



Prepared by Matt McKinney; Current as of 7/27/17

BrownWinick
ATTORNEYS AT LAW®
A Firm Commitment to Business™

DATA SECURITY AND PRIVACY LAWS

Updated July 2017

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

> **Personally Identifiable 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. Personal Information shall not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

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 BrownWinick's Data Security and Privacy Team.

Varying Definitions of Breach	
Gramm-Leach-Bliley Act (GLBA)	When a financial institution becomes aware of an incident of unauthorized access to sensitive customer information, the institution should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused. If the institution determines that misuse of its information about a customer has occurred or is reasonably possible, it should notify the affected customer as soon as possible. (12 C.F.R. § Pt. 30, App. B)
Health Insurance Portability and Accountability Act of 1996 (HIPAA)	The term "individually identifiable health information" means any information, including demographic information collected from an individual, that (A) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and-- (i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual. (42 U.S.C. § 1320d)
Alabama	No data security and privacy laws.
Alaska	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; in this paragraph, "acquisition" includes acquisition by (A) photocopying, facsimile, or other paper-based method; (B) a device, including a computer, that can read, write, or store information that is represented in numerical form; or (C) a method not identified by (A) or (B) of this paragraph; (Alaska Stat. § 45.48.090)
Arizona	When a person that conducts business in this state and that owns or licenses unencrypted computerized data that includes personal information becomes aware of an incident of unauthorized acquisition and access to unencrypted or unredacted computerized data that includes an individual's personal information, the person shall conduct a reasonable investigation to promptly determine if there has been a breach of the security system. If the investigation results in a determination that there has been a breach in the security system, the person shall notify the individuals affected. (Ariz. Rev. Stat. § 18-545)
Arkansas	Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person or business. (Ark. Code § 4-110-103)
California	Unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person, or, encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person and the person or business that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that personal information readable or useable. (Cal. Civ. Code § 1798.82)
Colorado	The unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an individual or a commercial entity. (C.R.S. § 6-1-716)

Varying Definitions of Breach	
Connecticut	The 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 (Conn. Gen. Stat. § 36a-701b)
Delaware	The unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an individual or a commercial entity. (Del. Code tit. 6, § 12B-101)
Florida	Unauthorized access of data in electronic form containing personal information. (F.S.A. § 501.171)
Georgia	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. (Ga. Code § 10-1-911)
Hawaii	An incident of unauthorized access to and acquisition of unencrypted or unredacted records or data containing personal information where illegal use of the personal information has occurred, or is reasonably likely to occur and that creates a risk of harm to a person. Any incident of unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential process or key constitutes a security breach. (Haw. Rev. Stat. § 487N-1)
Idaho	The illegal acquisition of unencrypted computerized data that materially compromises the security, confidentiality, or integrity of personal information for one (1) or more persons maintained by an agency, individual or a commercial entity. (Idaho Code § 28-51-104)
Illinois	Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the data collector. (815 Ill. Comp. Stat. 530/5)
Indiana	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. (Ind. Code § 24-4.9-2-2)
Iowa	The 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. (Iowa Code § 715C.1)
Kansas	The unauthorized access and acquisition of unencrypted or unredacted computerized data that compromises the security, confidentiality or integrity of personal information maintained by an individual or a commercial entity and that causes, or such individual or entity reasonably believes has caused or will cause, identity theft to any consumer. (Kan. Stat. § 50-7a01)

Varying Definitions of Breach	
Kentucky	Unauthorized acquisition of unencrypted and unredacted computerized data that compromises the security, confidentiality, or integrity of personally identifiable information maintained by the information holder as part of a database regarding multiple individuals that actually causes, or leads the information holder to reasonably believe has caused or will cause, identity theft or fraud against any resident of the Commonwealth of Kentucky. (Ky. Rev. Stat. § 365.732)
Louisiana	The compromise of the security, confidentiality, or integrity of computerized data that results in, or there is a reasonable basis to conclude has resulted in, the unauthorized acquisition of and access to personal information maintained by an agency or person. (La. Stat. § 51:3073)
Maine	The unauthorized acquisition, release or use of an individual's computerized data that includes personal information that compromises the security, confidentiality or integrity of personal information of the individual maintained by a person. (Me. Rev. Stat. tit. 10, § 1347)
Maryland	"Breach of the security of a system" means the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of the personal information maintained by a business. (Md. Code, Comm. Law § 14-3504)
Massachusetts	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. (Mass. Gen. Laws ch. 93H, § 1)
Michigan	The unauthorized access and acquisition of data that compromises the security or confidentiality of personal information maintained by a person or agency as part of a database of personal information regarding multiple individuals. (Mich. Comp. Laws § 445.63)
Minnesota	Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. (Minn. Stat. § 325E.61)
Mississippi	The unauthorized acquisition of electronic files, media, databases or computerized data containing personal information of any resident of this state when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable (Miss. Code. § 75-24-29)
Missouri	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. (Mo. Stat. § 407.1500)
Montana	Unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the person or business and causes or is reasonably believed to cause loss or injury to a Montana resident. (Mont. Code § 30-14-1704)
Nebraska	The unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an individual or a commercial entity. (Neb. Rev. St. § 87-802)

Varying Definitions of Breach	
Nevada	Unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information maintained by the data collector. (Nev. Rev. Stat. § 603A.020)
New Hampshire	Unauthorized acquisition of computerized data that compromises the security or confidentiality of personal information maintained by a person doing business in this state. (N.H. Rev. Stat. § 359-C:19)
New Jersey	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. (N.J. Stat. § 56:8-161)
New Mexico	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. (N.M. HB 15 § 2)
New York	Unauthorized acquisition or acquisition without valid authorization of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a business. (N.Y. Gen. Bus. Law § 899-aa)
North Carolina	An incident of unauthorized access to and acquisition of unencrypted and unredacted records or data containing personal information where illegal use of the personal information has occurred or is reasonably likely to occur or that creates a material risk of harm to a consumer. Any incident of unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential process or key shall constitute a security breach. (N.C. Gen. Stat. § 75-61)
North Dakota	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. (NDCC § 51-30-01)
Ohio	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. (R.C. § 1349.19)
Oklahoma	The unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes, or the individual or entity reasonably believes has caused or will cause, identity theft or other fraud to any resident of this state. (24 Okl.St. § 162)
Oregon	An unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information that a person maintains. (O.R.S. § 646A.602)
Pennsylvania	The unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of personal information maintained by the entity as part of a database of personal information regarding multiple individuals and that causes or the entity reasonably believes has caused or will cause loss or injury to any resident of this Commonwealth. (73 Pa. Stat. § 2302)

Varying Definitions of Breach	
Rhode Island	Unauthorized access or acquisition of unencrypted, computerized data information that compromises the security, confidentiality, or integrity of personal information maintained by the municipal agency, state agency, or person. (11 R.I. Gen. Laws § 11-49.3-3)
South Carolina	Unauthorized access to and acquisition of computerized data that was not rendered unusable through encryption, redaction, or other methods that compromises the security, confidentiality, or integrity of personal identifying information maintained by the person, when illegal use of the information has occurred or is reasonably likely to occur or use of the information creates a material risk of harm to a resident. (Code 1976 § 39-1-90)
South Dakota	No data security and privacy laws.
Tennessee	The acquisition of unencrypted computerized data or encrypted computerized data and the encryption key by an unauthorized person that materially compromises the security, confidentiality, or integrity of personal information maintained by the information holder. (Tenn. Code § 47-18-2107)
Texas	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. (Tex. Bus. & Com. Code § 521.053)
Utah	An unauthorized acquisition of computerized data maintained by a person that compromises the security, confidentiality, or integrity of personal information. (U.C. 1953 § 13-44-102)
Vermont	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. (9 V.S. § 2430)
Virginia	The unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes, or the individual or entity reasonably believes has caused, or will cause, identity theft or other fraud to any resident of the Commonwealth. (VA Code § 18.2-186.6)
Washington	Unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. (Wash. Rev. Code § 19.255.010)
West Virginia	The unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes the individual or entity to reasonably believe that the breach of security has caused or will cause identity theft or other fraud to any resident of this state. (W. Va. Code, § 46A-2A-101)
Wisconsin	Acquisition of personal information maintained or licensed by the entity by an unauthorized person. (W.S. § 134.98)
Wyoming	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. (W.S.1977 § 40-12-501)

Varying Definitions of Breach	
District of Columbia	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. Acquisition of data that has been rendered secure, so as to be unusable by an unauthorized third party, shall not be deemed to be a breach of the security of the system. (DC ST § 28-3851)
Puerto Rico	The term "breach" is not defined. (10 L.P.R. § 4051)

Varying Definitions of Personally Identifiable Information (PII)	
Gramm-Leach-Bliley Act (GLBA)	The term "nonpublic personal information" means personally identifiable financial information-- (i) provided by a consumer to a financial institution; (ii) resulting from any transaction with the consumer or any service performed for the consumer; or (iii) otherwise obtained by the financial institution. (B) Such term does not include publicly available information, as such term is defined by the regulations prescribed under section 6804 of this title. (C) Notwithstanding subparagraph (B), such term-- (i) shall include any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any nonpublic personal information other than publicly available information; but (ii) shall not include any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived without using any nonpublic personal information. (15 U.S.C. § 6809)
Health Insurance Portability and Accountability Act of 1996 (HIPAA)	The term "individually identifiable health information" means any information, including demographic information collected from an individual, that (A) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and-- (i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual. (42 U.S.C. § 1320d)
Alabama	No data security and privacy laws.
Alaska	Personal Information of Alaska residents. Standard definition, plus: passwords, personal identification numbers, or other access codes for financial accounts. (Alaska Stat. § 45.48.090)
Arizona	See standard definition above. (Ariz. Rev. Stat. § 18-54)
Arkansas	Personal Information of Arkansas residents. In addition: medical information. (Ark. Code § 4-110-103).

Varying Definitions of Personally Identifiable Information (PII)	
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; medical information and health insurance information. (Cal. Civ. Code § 1798.81.5) 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. (Cal. Civ. Code § 1798.81.5)
Colorado	Personal information of Colorado residents. See standard definition above. (C.R.S.A. § 6-1-716)
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). (C.G.S.A. § 36a-701b)
Delaware	Personal information of Delaware residents. See standard definition above. (6 Del.C. § 12B-101)
Florida	Personal Information means either of the following: a. An individual's first name or first initial and last name in combination with any one or more of the following data elements for that individual: (i) a social security number; (ii) a driver license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity; (iii) a financial account number or credit or debit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual's financial account; (iv) any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or (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. (F.S.A. § 501.171)
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. (Ga. Code § 10-1-911)

Varying Definitions of Personally Identifiable Information (PII)	
Hawaii	Personal information of Hawaii residents. See standard definition above. (HRS § 487N-1)
Idaho	Personal information of Idaho residents. See standard definition above. (I.C. § 28-51-104)
Illinois	"Personal information" means either of the following: (1) an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the name or data elements have been acquired without authorization through the breach of security: (A) Social Security number. (B) Driver's license number or State identification card number. (C) Account number or credit or debit card number, or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account. (D) Medical information. (E) Health insurance information. (F) Unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee to authenticate an individual, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data. (2) user name or email address, in combination with a password or security question and answer that would permit access to an online account, when either the user name or email address or password or security question and answer are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the data elements have been obtained through the breach of security. (815 ILCS § 530/5)
Indiana	"Personal information" means: (1) a Social Security number that is not encrypted or redacted; or (2) an individual's first and last names, or first initial and last name, and one (1) or more of the following data elements that are not encrypted or redacted: (A) A driver's license number. (B) A state identification card number. (C) A credit card number. (D) A financial account number or debit card number in combination with a security code, password, or access code that would permit access to the person's account. (Ind. Code § 24-4.9-2-10)
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. (I.C.A. § 715C.1)
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. (K.S.A. § 50-7a01)
Kentucky	See standard definition above. (KRS § 365.732)
Louisiana	See standard definition above. (LSA-R.S. § 51:3073)

Varying Definitions of Personally Identifiable Information (PII)	
Maine	Personal Information of Maine residents. In addition: a password, if any of the other data elements alone would be sufficient to permit a person to fraudulently assume or attempt to assume the identity of the person whose information was compromised. (10 M.R.S.A. § 1347)
Maryland	(i) An individual's first name or first initial and last name in combination with any one or more of the following data elements, when the name or the data elements are not encrypted, redacted, or otherwise protected by another method that renders the information unreadable or unusable: 1. A Social Security number, an Individual Taxpayer Identification Number, a passport number, or other identification number issued by the federal government; 2. 2. A driver's license number or State identification card number;(iii) 3. A financial An account number, including a credit card number, or a debit card number, that in combination with any required security code, access code, or password, would permit that permits access to an individual's financial account; or 4. An Individual Taxpayer Identification Number Health information, including information about an individual's mental health; 5. A health insurance policy or certificate number or health insurance subscriber identification number, in combination with a unique identifier used by an insurer or an employer that is self-insured, that permits access to an individual's health information; or 6. Biometric data of an individual generated by automatic measurements of an individual's biological characteristics such as a fingerprint, voice print, genetic print, retina or iris image, or other unique biological characteristic, that can be used to uniquely authenticate the individual's identity when the individual accesses a system or account; or (ii) A user name or e-mail address in combination with a password or security question and answer that permits access to an individual's e-mail account. (Md. Code, Comm. Law § 14-3501)
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. (M.G.L.A. 93H § 1)
Michigan	Personal information of Michigan residents. See standard definition above. (M.C.L.A. § 445.63)
Minnesota	See standard definition above. (M.S.A. § 325E.61)
Mississippi	See standard definition above. (Miss. Code § 75-24-29)
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. (V.A.M.S. § 407.1500)

Varying Definitions of Personally Identifiable Information (PII)	
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). (MCA § 30-14-1702)
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. (Neb. Rev. St. § 87-802)
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. (N.R.S. 603A.040)
New Hampshire	Personal information of New Hampshire residents. See standard definition above. (N.H. Rev. Stat. § 359-C:19)
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. (N.J.S. § 56:8-161)
New Mexico	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. (N.M. HB 15 § 2)

Varying Definitions of Personally Identifiable Information (PII)	
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. (N.Y. Gen. Bus. Law § 899-aa)
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) biometric data; (5) finger prints; (6) 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 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. (N.C.G.S. § 75-61)
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. (NDCC § 51-30-01)

Varying Definitions of Personally Identifiable Information (PII)	
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. (R.C. § 1349.19)
Oklahoma	See standard definition above. (24 Okl.St. § 162)
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 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. (O.R.S. § 646A.602)
Pennsylvania	See standard definition above. (73 P.S. § 2302)

Varying Definitions of Personally Identifiable Information (PII)	
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. (11 R.I. Gen. Laws § 11-49.3-3)
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. (Code 1976 § 39-1-90)
South Dakota	No data security and privacy laws.
Tennessee	See standard definition above. (T. C. A. § 47-18-2107)
Texas	Information that alone or in conjunction with other information identifies an individual, including an individual's: (A) name, social security number, date of birth, or government-issued identification number; (B) mother's maiden name; (C) unique biometric data, including the individual's fingerprint, voice print, and retina or iris image; (D) unique electronic identification number, address, or routing code; and (E) telecommunication access device as defined by Section 32.51, Penal Code. (Tex. Bus. & Com. Code § 521.002)
Utah	See standard definition above. (U.C.A. 1953 § 13-44-102)
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 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. (9 V.S.A. § 2430)

Varying Definitions of Personally Identifiable Information (PII)	
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. (VA Code § 18.2-186.6)
Washington	See standard definition above. (Wash. Rev. Code § 19.255.010)
West Virginia	See standard definition above. (W. Va. Code, § 46A-2A-101)
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. (W.S.A. § 134.98)
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; (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. (W.S.1977 § 40-12-501)

Varying Definitions of Personally Identifiable Information (PII)	
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. (DC ST § 28-3851)
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. (10 L.P.R.A. § 4051)

Entities Covered by the Statute	
Gramm-Leach-Bliley Act (GLBA)	(A) national banks, Federal branches and Federal agencies of foreign banks, and any subsidiaries of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers); (B) member banks of the Federal Reserve System (other than national banks), branches and agencies of foreign banks (other than Federal branches, Federal agencies, and insured State branches of foreign banks), commercial lending companies owned or controlled by foreign banks, organizations operating under section 25 or 25A of the Federal Reserve Act [12 U.S.C.A. § 601 et seq. or 611 et seq.], and bank holding companies and their nonbank subsidiaries or affiliates (except brokers, dealers, persons providing insurance, investment companies, and investment advisers); (C) banks insured by the Federal Deposit Insurance Corporation (other than members of the Federal Reserve System), insured State branches of foreign banks, and any subsidiaries of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers); and (D) savings associations the deposits of which are insured by the Federal Deposit Insurance Corporation, and any subsidiaries of such savings associations (except brokers, dealers, persons providing insurance, investment companies, and investment advisers). (U.S.C. § 6805)

Entities Covered by the Statute	
Health Insurance Portability and Accountability Act of 1996 (HIPAA)	Health plan, health care clearinghouse, and health care provider who transmits any health information in electronic form in connection with a transaction referred to in section 1320d-2(a)(1) of this title. (42 U.S.C. § 1320d-1)
Alaska	If a covered person owns or licenses personal information in any form that includes personal information on a state resident, and a breach of the security of the information system that contains personal information occurs, the covered person shall, after discovering or being notified of the breach, disclose the breach to each state resident whose personal information was subject to the breach. (Alaska Stat. § 45.48.010). "Covered person" means a (A) person doing business; (B) governmental agency; or (C) person with more than 10 employees "Information collector" means a covered person who owns or licenses personal information in any form if the personal information includes personal information on a state resident (AS § 45.48.090)
Arizona	"Person" means a natural person, corporation, business trust, estate, trust, partnership, association, joint venture, government, governmental subdivision or agency or any other legal or commercial entity. Person does not include the department of public safety, a county sheriff's department, a municipal police department, a prosecution agency or a court. (A.R.S. § 18-545).
Arkansas	Any person or business that acquires, owns, or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach of the security of the system to any resident of Arkansas whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. (Ark. Code § 4-110-105). "Business" means a sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the law of this state, any other state, the United States, or of any other country or the parent or the subsidiary of a financial institution. "Individual" means a natural person. (Ark. Code § 4-110-103)
California	A person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. (Cal. Civ. Code § 1798.82) "Business" means a sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the law of this state, any other state, the United States, or of any other country, or the parent or the subsidiary of a financial institution. The term includes an entity that disposes of records. "Individual" means a natural person. (Cal. Civ. Code § 1798.80)

Entities Covered by the Statute	
Colorado	An individual or a commercial entity that conducts business in Colorado and that owns or licenses computerized data that includes personal information about a resident of Colorado shall, when it becomes aware of a breach of the security of the system, conduct in good faith a prompt investigation to determine the likelihood that personal information has been or will be misused. "Commercial entity" means any private legal entity, whether for-profit or not-for-profit. (C.R.S.A. § 6-1-716)
Connecticut	Any person who conducts business in this state, and who, in the ordinary course of such person's business, owns, licenses or maintains computerized data that includes personal information. Any person that maintains computerized data that includes personal information that the person does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following its discovery, if the personal information of a resident of this state was breached or is reasonably believed to have been breached. (Conn. Gen. Stat. § 36a-701b).
Delaware	An individual or a commercial entity that conducts business in Delaware and that owns or licenses computerized data that includes personal information about a resident of Delaware shall, when it becomes aware of a breach of the security of the system, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused. If the investigation determines that the misuse of information about a Delaware resident has occurred or is reasonably likely to occur, the individual or the commercial entity shall give notice as soon as possible to the affected Delaware resident. An individual or a commercial entity that maintains computerized data that includes personal information that the individual or the commercial entity does not own or license shall give notice to and cooperate with the owner or licensee of the information of any breach of the security of the system immediately following discovery of a breach, if misuse of personal information about a Delaware resident occurred or is reasonably likely to occur. (Del. Code tit. 6, § 12B-102)
Florida	A covered entity shall provide notice to the department of any breach of security affecting 500 or more individuals in this state. "Covered entity" means a sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity that acquires, maintains, stores, or uses personal information. (Fla. Stat. § 501.171)

Entities Covered by the Statute	
Georgia	Any information broker or data collector that maintains computerized data that includes personal information of individuals shall give notice of any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. (Ga. Code § 10-1-912) "Data collector" means any state or local agency or subdivision thereof including any department, bureau, authority, public university or college, academy, commission, or other government entity; provided, however, that the term "data collector" shall not include any governmental agency whose records are maintained primarily for traffic safety, law enforcement, or licensing purposes or for purposes of providing public access to court records or to real or personal property information. "Information broker" means any person or entity who, for monetary fees or dues, engages in whole or in part in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring, or communicating information concerning individuals for the primary purpose of furnishing personal information to nonaffiliated third parties, but does not include any governmental agency whose records are maintained primarily for traffic safety, law enforcement, or licensing purposes. (Ga. Code § 10-1-911)
Hawaii	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 shall provide notice to the affected person that there has been a security breach following discovery or notification of the breach. (Haw. Rev. Stat. § 487N-2) "Business" means a sole proprietorship, partnership, corporation, association, or other group, however organized, and whether or not organized to operate at a profit. The term includes a financial institution organized, chartered, or holding a license or authorization certificate under the laws of the State, any other state, the United States, or any other country, or the parent or the subsidiary of any such financial institution. (Haw. Rev. Stat. § 487N-1)

Entities Covered by the Statute	
Idaho	A city, county or state agency, individual or a commercial entity that conducts business in Idaho and that owns or licenses computerized data that includes personal information about a resident of Idaho shall, when it becomes aware of a breach of the security of the system, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused. If the investigation determines that the misuse of information about an Idaho resident has occurred or is reasonably likely to occur, the agency, individual or the commercial entity shall give notice as soon as possible to the affected Idaho resident. An agency, individual or a commercial entity that maintains computerized data that includes personal information that the agency, individual or the commercial entity does not own or license shall give notice to and cooperate with the owner or licensee of the information of any breach of the security of the system immediately following discovery of a breach if misuse of personal information about an Idaho resident occurred or is reasonably likely to occur. Cooperation includes sharing with the owner or licensee information relevant to the breach. (Idaho Code § 28-51-105)
Illinois	Any data collector that owns or licenses personal information concerning an Illinois resident shall notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach. (815 Ill. Comp. Stat. 530/10) “Data Collector” may include, but is not limited to, government agencies, public and private universities, privately and publicly held corporations, financial institutions, retail operators, and any other entity that, for any purpose, handles, collects, disseminates, or otherwise deals with nonpublic personal information. (815 Ill. Comp. Stat. 530/5)
Indiana	Except as provided in section 4(c), 4(d), and 4(e) of this chapter, after discovering or being notified of a breach of the security of data, the data base owner shall disclose the breach to an Indiana resident whose: (1) unencrypted personal information was or may have been acquired by an unauthorized person; or (2) encrypted personal information was or may have been acquired by an unauthorized person with access to the encryption key; if the data base owner knows, should know, or should have known that the unauthorized acquisition constituting the breach has resulted in or could result in identity deception (as defined in IC 35-43-5-3.5), identity theft, or fraud affecting the Indiana resident. (Ind. Code § 24-4.9-3-1) “Data base owner” means a person that owns or licenses computerized data that includes personal information. (Ind. Code § 24-4.9-2-3)

Entities Covered by the Statute	
Iowa	Any person who owns or licenses computerized data that includes a consumer's personal information that is used in the course of the person's business, vocation, occupation, or volunteer activities and that was subject to a breach of security shall give notice of the breach of security following discovery of such breach of security, or receipt of notification under subsection 2, to any consumer whose personal information was included in the information that was breached. (Iowa Code § 715C.2) "Person" means an individual; corporation; business trust; estate; trust; partnership; limited liability company; association; joint venture; government; governmental subdivision, agency, or instrumentality; public corporation; or any other legal or commercial entity. "Consumer" means an individual who is a resident of this state. (Iowa Code § 715C.1)
Kansas	A person that conducts business in this state, or a government, governmental subdivision or agency that owns or licenses computerized data that includes personal information 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. (Kan. Stat. § 50-7a02) "Person" means any individual, partnership, corporation, trust, estate, cooperative, association, government, or governmental subdivision or agency or other entity. (Kan. Stat. § 50-7a01)
Kentucky	Any information holder shall disclose any breach of the security of the system, following discovery or notification of the breach in the security of the data, to any resident of Kentucky whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. "Information holder" means any person or business entity that conducts business in this state. (Ky. Rev. Stat. § 365.732)
Louisiana	Any person that conducts business in the state or that owns or licenses computerized data that includes personal information, or any agency that owns or licenses computerized data that includes personal information, shall, following discovery of a breach in the security of the system containing such data, notify any resident of the state whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person. (La. Stat. § 51:3074) "Person" means any individual, corporation, partnership, sole proprietorship, joint stock company, joint venture, or any other legal entity. (La. Stat. § 51:3073)

Entities Covered by the Statute	
Maine	If an information broker that maintains computerized data that includes personal information becomes aware of a breach of the security of the system, the information broker shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused and shall give notice of a breach of the security of the system following discovery or notification of the security breach to a resident of this State whose personal information has been, or is reasonably believed to have been, acquired by an unauthorized person. If any other person who maintains computerized data that includes personal information becomes aware of a breach of the security of the system, the person shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused and shall give notice of a breach of the security of the system following discovery or notification of the security breach to a resident of this State if misuse of the personal information has occurred or if it is reasonably possible that misuse will occur. (Me. Rev. Stat. tit. 10, § 1348) “Information broker” means a person who, for monetary fees or dues, engages in whole or in part in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring or communicating information concerning individuals for the primary purpose of furnishing personal information to nonaffiliated 3rd parties. “Person” means an individual, partnership, corporation, limited liability company, trust, estate, cooperative, association or other entity, including agencies of State Government, the University of Maine System, the Maine Community College System, Maine Maritime Academy and private colleges and universities. (Me. Rev. Stat. tit. 10, § 1347)
Maryland	A business that owns or licenses computerized data that includes personal information of an individual residing in the State, when it discovers or is notified of a breach of the security of a system, shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information of the individual has been or will be misused as a result of the breach. If, after the investigation is concluded, the business determines that misuse of the individual's personal information has occurred or is reasonably likely to occur as a result of a breach of the security of a system, the business shall notify the individual of the breach. (Md. Code , Com. Law § 14-3504) “Business” means a sole proprietorship, partnership, corporation, association, or any other business entity, whether or not organized to operate at a profit. (Md. Code , Com. Law § 14-3501)

Entities Covered by the Statute	
Massachusetts	A person or agency that maintains or stores, but does not own or license data that includes personal information about a resident of the commonwealth, shall provide notice, as soon as practicable and without unreasonable delay, when such person or agency (1) knows or has reason to know of a breach of security or (2) when the person or agency knows or has reason to know that the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose, to the owner or licensor in accordance with this chapter. (Mass. Gen. Laws ch. 93H, § 3) "Person", a natural person, corporation, association, partnership or other legal entity. (Mass. Gen. Laws ch. 93H, § 1)
Michigan	Unless the person or agency determines that the security breach has not or is not likely to cause substantial loss or injury to, or result in identity theft with respect to, 1 or more residents of this state, a person or agency that owns or licenses data that are included in a database that discovers a security breach, or receives notice of a security breach under subsection (2), shall provide a notice of the security breach to each resident of this state who meets 1 or more of the following: (a) That resident's unencrypted and unredacted personal information was accessed and acquired by an unauthorized person. (b) That resident's personal information was accessed and acquired in encrypted form by a person with unauthorized access to the encryption key. (Mich. Comp. Laws § 445.72) "Person" means an individual, partnership, corporation, limited liability company, association, or other legal entity. (Mich. Comp. Laws § 445.63)
Minnesota	Any person or business that conducts business in this state, and that owns or licenses data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Any person or business that maintains data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. (Minn. Stat. § 325E.61)
Mississippi	This section applies to any person who conducts business in this state and who, in the ordinary course of the person's business functions, owns, licenses or maintains personal information of any resident of this state. (Miss. Code. § 75-24-29). "Person" means natural persons, corporations, trusts, partnerships, incorporated and unincorporated associations, and any other legal entity. (Miss. Code. § 75-24-3)

Entities Covered by the Statute	
Missouri	Any person that owns or licenses personal information of residents of Missouri or any person that conducts business in Missouri that owns or licenses personal information in any form of a resident of Missouri shall provide notice to the affected consumer that there has been a breach of security following discovery or notification of the breach. “Person”, any individual, corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture, government, governmental subdivision, governmental agency, governmental instrumentality, public corporation, or any other legal or commercial entity. (Mo. Stat. § 407.1500)
Montana	Any person or business that conducts business in Montana and that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the data system following discovery or notification of the breach to any resident of Montana whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data system immediately following discovery if the personal information was or is reasonably believed to have been acquired by an unauthorized person. (Mont. Code § 30-14-1704) “Business” means a sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the law of this state, any other state, the United States, or any other country or the parent or the subsidiary of a financial institution. (Mont. Code § 30-14-1702)

Entities Covered by the Statute	
Nebraska	An individual or a commercial entity that conducts business in Nebraska and that owns or licenses computerized data that includes personal information about a resident of Nebraska shall, when it becomes aware of a breach of the security of the system, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be used for an unauthorized purpose. If the investigation determines that the use of information about a Nebraska resident for an unauthorized purpose has occurred or is reasonably likely to occur, the individual or commercial entity shall give notice to the affected Nebraska resident. An individual or a commercial entity that maintains computerized data that includes personal information that the individual or commercial entity does not own or license shall give notice to and cooperate with the owner or licensee of the information of any breach of the security of the system when it becomes aware of a breach if use of personal information about a Nebraska resident for an unauthorized purpose occurred or is reasonably likely to occur. (Neb. Rev. Stat. § 87-803). Commercial entity includes a corporation, business trust, estate, trust, partnership, limited partnership, limited liability partnership, limited liability company, association, organization, joint venture, government, governmental subdivision, agency, or instrumentality, or any other legal entity, whether for profit or not for profit. (Neb. Rev. Stat. § 87-802)
Nevada	Any data collector that owns or licenses computerized data which includes personal information shall disclose any breach of the security of the system data following discovery or notification of the breach to any resident of this State whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. (Nev. Rev. Stat. § 603A. 220) “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. (Nev. Rev. Stat. § 603A.030)

Entities Covered by the Statute	
New Hampshire	(a) Any person doing business in this state who owns or licenses computerized data that includes personal information shall, when it becomes aware of a security breach, promptly determine the likelihood that the information has been or will be misused. If the determination is that misuse of the information has occurred or is reasonably likely to occur, or if a determination cannot be made, the person shall notify the affected individuals as soon as possible as required under this subdivision. (b) Any person engaged in trade or commerce that is subject to RSA 358-A:3, I shall also notify the regulator which has primary regulatory authority over such trade or commerce. All other persons shall notify the New Hampshire attorney general's office. (c) Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify and cooperate with the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was acquired by an unauthorized person. (N.H. Rev. Stat. § 359-C:20) "Person" means an individual, corporation, trust, partnership, incorporated or unincorporated association, limited liability company, or other form of entity, or any agency, authority, board, court, department, division, commission, institution, bureau, or other state governmental entity, or any political subdivision of the state. (N.H. Rev. Stat. § 359-C:19)
New Jersey	Any business that conducts business in New Jersey, or any public entity that compiles or maintains computerized records that include personal information, shall disclose any breach of security of those computerized records following discovery or notification of the breach to any customer who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person. Any business or public entity that compiles or maintains computerized records that include personal information on behalf of another business or public entity shall notify that business or public entity, who shall notify its New Jersey customers, as provided in subsection a. of this section, of any breach of security of the computerized records immediately following discovery, if the personal information was, or is reasonably believed to have been, accessed by an unauthorized person. (N.J. Stat. § 56:8-163) "Business" means a sole proprietorship, partnership, corporation, association, or other entity, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the law of this State, any other state, the United States, or of any other country, or the parent or the subsidiary of a financial institution. (N.J. Stat. § 56:8-161)
New Mexico	Any "person," which includes an individual, corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture or any legal or commercial entity. (N.M. HB 15) (N.M. Stat. § 12-2A-3) or commercial entity

Entities Covered by the Statute	
New York	Any person or business which conducts business in New York state, and which owns or licenses computerized data which includes private information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of New York state whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision four of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system. Any person or business which maintains computerized data which includes private information which such person or business does not own shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the private information was, or is reasonably believed to have been, acquired by a person without valid authorization. (N.Y. Gen. Bus. Law § 899-aa)
North Carolina	Any business that owns or licenses personal information of residents of North Carolina or any business that conducts business in North Carolina that owns or licenses personal information in any form (whether computerized, paper, or otherwise) shall provide notice to the affected person that there has been a security breach following discovery or notification of the breach. (N.C. Gen. Stat. § 75-65) “Business”. -- A sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not organized to operate at a profit. The term includes a financial institution organized, chartered, or holding a license or authorization certificate under the laws of this State, any other state, the United States, or any other country, or the parent or the subsidiary of any such financial institution. Business shall not include any government or governmental subdivision or agency. (N.C. Gen. Stat. § 75-61)
North Dakota	Any person that owns or licenses computerized data that includes personal information, shall disclose any breach of the security system following discovery or notification of the breach in the security of the data to any resident of the state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. (N.D. Cent. Code § 51-30-02)
Ohio	Any person that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system, following its discovery or notification of the breach of the security of the system, to any resident of this state whose personal information was, or reasonably is believed to have been, accessed and acquired by an unauthorized person if the access and acquisition by the unauthorized person causes or reasonably is believed will cause a material risk of identity theft or other fraud to the resident. “Person” has the same meaning as in section 1.59 of the Revised Code, except that “person” includes a business entity only if the business entity conducts business in this state. (Ohio Rev. Code § 1349.19)

Entities Covered by the Statute	
Oklahoma	An individual or entity that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach of the security of the system to any resident of this state whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person and that causes, or the individual or entity reasonably believes has caused or will cause, identity theft or other fraud to any resident of this state. (Okla. Stat. tit. 24, § 163) "Entity" includes corporations, business trusts, estates, partnerships, limited partnerships, limited liability partnerships, limited liability companies, associations, organizations, joint ventures, governments, governmental subdivisions, agencies, or instrumentalities, or any other legal entity, whether for profit or not-for-profit. (Okla. Stat. tit. 24, § 162)
Oregon	A person that owns or licenses personal information that the person uses in the course of the person's business, vocation, occupation or volunteer activities and that was subject to a breach of security shall give notice of the breach of security to: The consumer to whom the personal information pertains after the person discovers the breach of security or after the person receives notice of a breach of security under subsection (2) of this section. (Or. Rev. Stat. § 646A. 604) "Person" means an individual, private or public corporation, partnership, cooperative, association, estate, limited liability company, organization or other entity, whether or not organized to operate at a profit, or a public body as defined in ORS 174.109. (Or. Rev. Stat. § 646A.602)
Pennsylvania	An entity that maintains, stores or manages computerized data that includes personal information shall provide notice of any breach of the security of the system following discovery of the breach of the security of the system to any resident of this Commonwealth whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person. (73 Pa. Stat. § 2303) A State agency, a political subdivision of the Commonwealth or an individual or a business doing business in this Commonwealth. (73 Pa. Stat. § 2302)
Rhode Island	Any municipal agency, state agency or person that stores, owns, collects, processes, maintains, acquires, uses or licenses data that includes personal information, shall provide notification as set forth in this section of any disclosure of personal information, or any breach of the security of the system, which poses a significant risk of identity theft to any resident of Rhode Island whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person or entity. "Person" shall include any individual, sole proprietorship, partnership, association, corporation, or joint venture, business or legal entity, trust, estate, cooperative or other commercial entity. (11 R.I. Gen. Laws § 11-49.3-4)

Entities Covered by the Statute	
South Carolina	A person conducting business in this State, and owning or licensing computerized data or other data that includes personal identifying information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of this State whose personal identifying information that was not rendered unusable through encryption, redaction, or other methods was, or is reasonably believed to have been, acquired by an unauthorized person when the illegal use of the information has occurred or is reasonably likely to occur or use of the information creates a material risk of harm to the resident. (S.C. Code § 39-1-90) "Person" includes a natural person or an individual, and an organization. "Organization" means a corporation, government or governmental subdivision or agency, trust, estate, partnership, cooperative or association. (S.C. Code § 37-1-301)
South Dakota	No data security notification laws.
Tennessee	Any information holder shall disclose any breach of the security of the system, following discovery or notification of the breach in the security of the data, to any resident of Tennessee whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person. "Information holder" means any person or business that conducts business in this state, or any agency of the state of Tennessee or any of its political subdivisions, that owns or licenses computerized data that includes personal information. (Tenn. Code § 47-18-2107).
Texas	A person who conducts business in this state and owns or licenses computerized data that includes sensitive personal information shall disclose any breach of system security, after discovering or receiving notification of the breach, to any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person. (Tex. Bus. & Com. Code § 521.053)
Utah	A person who owns or licenses computerized data that includes personal information concerning a Utah resident shall, when the person becomes aware of a breach of system security, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused for identity theft or fraud purposes. If an investigation under Subsection (1)(a) reveals that the misuse of personal information for identity theft or fraud purposes has occurred, or is reasonably likely to occur, the person shall provide notification to each affected Utah resident. (Utah Code § 13-44-202) "Person" means an individual, association, institution, corporation, company, trust, limited liability company, partnership, political subdivision, government office, department, division, bureau, or other body of government, and any other organization or entity. (Utah Code § 68-3-12.5)

Entities Covered by the Statute	
Vermont	Any data collector that owns or licenses computerized personally identifiable information that includes personal information concerning a consumer shall notify the consumer that there has been a security breach following discovery or notification to the data collector of the breach. (Vt. Stat. tit. 9, § 2435). "Data collector" may include the State, State agencies, political subdivisions of the State, public and private universities, privately and publicly held corporations, limited liability companies, financial institutions, retail operators, and any other entity that, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates, or otherwise deals with nonpublic personal information. (Vt. Stat. tit. 9, § 2430)
Virginia	If unencrypted or unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person and causes, or the individual or entity reasonably believes has caused or will cause, identity theft or another fraud to any resident of the Commonwealth, an individual or entity that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach of the security of the system to the Office of the Attorney General and any affected resident of the Commonwealth without unreasonable delay. "Individual" means a natural person. "Entity" includes corporations, business trusts, estates, partnerships, limited partnerships, limited liability partnerships, limited liability companies, associations, organizations, joint ventures, governments, governmental subdivisions, agencies, or instrumentalities or any other legal entity, whether for profit or not for profit. (Va. Code § 18.2-186.6)
Washington	Any person or business that conducts business in this state and that owns or licenses data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the personal information was not secured. Any person or business that maintains data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. (Wash. Rev. Code § 19.255.010)

Entities Covered by the Statute	
West Virginia	An individual or entity that owns or licenses computerized data that includes personal information shall give notice of any breach of the security of the system following discovery or notification of the breach of the security of the system to any resident of this state whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person and that causes, or the individual or entity reasonably believes has caused or will cause, identity theft or other fraud to any resident of this state. (W. Va. Code § 46A-2A-102) "Entity" includes corporations, business trusts, estates, partnerships, limited partnerships, limited liability partnerships, limited liability companies, associations, organizations, joint ventures, governments, governmental subdivisions, agencies or instrumentalities, or any other legal entity, whether for profit or not for profit. (W. Va. Code § 46A-2A-101)
Wisconsin	If an entity whose principal place of business is located in this state or an entity that maintains or licenses personal information in this state knows that personal information in the entity's possession has been acquired by a person whom the entity has not authorized to acquire the personal information, the entity shall make reasonable efforts to notify each subject of the personal information. The notice shall indicate that the entity knows of the unauthorized acquisition of personal information pertaining to the subject of the personal information. If an entity whose principal place of business is not located in this state knows that personal information pertaining to a resident of this state has been acquired by a person whom the entity has not authorized to acquire the personal information, the entity shall make reasonable efforts to notify each resident of this state who is the subject of the personal information. "Entity" means a person, other than an individual, that does any of the following: a. Conducts business in this state and maintains personal information in the ordinary course of business. b. Licenses personal information in this state. c. Maintains for a resident of this state a depository account as defined in s. 815.18(2)(e). d. Lends money to a resident of this state. (Wis. Stat. § 134.98)
Wyoming	An individual or commercial entity that conducts business in Wyoming and that owns or licenses computerized data that includes personal identifying information about a resident of Wyoming shall, when it becomes aware of a breach of the security of the system, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal identifying information has been or will be misused. If the investigation determines that the misuse of personal identifying information about a Wyoming resident has occurred or is reasonably likely to occur, the individual or the commercial entity shall give notice as soon as possible to the affected Wyoming resident. (Wyo. Stat. § 40-12-502)
District of Columbia	Any person or entity who conducts business in the District of Columbia, and who, in the course of such business, owns or licenses computerized or other electronic data that includes personal information, and who discovers a breach of the security of the system, shall promptly notify any District of Columbia resident whose personal information was included in the breach. (D.C. Code § 28-3852)

Entities Covered by the Statute	
Puerto Rico	Any entity that is the owner or custodian of a database that includes personal information of citizens residents of Puerto Rico must notify said citizens of any breach of the security of the system when the database whose security has been breached contains, in whole or in part, personal information files and the same are not protected by an encrypted code but only by a password. (10 L.P.R.A. § 4052) Entity. Means every agency, board, body, examining board, corporation, public corporation, committee, independent office, division, administration, bureau, department, authority, official, instrumentality or administrative organism of the three branches of the Government; every corporation, partnership, association, private company or organization authorized to do business or operate in the Commonwealth of Puerto Rico; as well as every public or private educational institution, regardless of the level of education offered by it. (10 L.P.R.A. § 4051)

Encryption Safe Harbor	
Gramm-Leach-Bliley Act (GLBA)	No encryption safe harbor.
Health Insurance Portability and Accountability Act of 1996 (HIPAA)	No encryption safe harbor.
Alaska	The statute only applies to unencrypted information or encrypted information when the encryption key has also been disclosed. (Alaska Stat. § 45.48.090)
Arizona	Notification requirement applies when the personal information is readable. (A.R.S. § 18-545).
Arkansas	Statute only applies to unencrypted data elements. (Ark. Code §§ 4-110-103, -105)
California	Notification is needed when unencrypted information is reasonably believed to have been acquired or when encrypted information is reasonably believed to have been acquired along with the encryption key. (Cal. Civ. Code § 1798.82)
Colorado	Statute applies only to the disclosure of unencrypted computerized data. (Colo. Rev. Stat. § 6-1-716)
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. (Conn. Gen. Stat. § 36a-701b)
Delaware	Statute applies to unencrypted computerized data. (Del. Code tit. 6, § 12B-101)
Florida	The statute applies to unencrypted information. (Fla. Stat. § 501.171(g)(2))

Encryption Safe Harbor	
Georgia	The statute applies to unencrypted personal information. (Ga. Code § 10-1-911).
Hawaii	Statute applies to disclosure of unencrypted or unredacted information and also encrypted data if the encryption key is acquired. (Haw. Rev. Stat. § 487N-1)
Idaho	Statute applies to unencrypted personal information. (Idaho Code § 28-51-104)
Illinois	The statute applies to unencrypted personal information and also encrypted data if the security key has been acquired. (815 Ill. Comp. Stat. 530/5)
Indiana	The applies to unencrypted data and encrypted data when the security key has access to the security key. (Ind. Code § 24-4.9-3-1)
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. (Iowa Code § 715C.1)
Kansas	The statute is triggered by disclosure of unencrypted or unredacted information. (Kan. Stat. § 50-7a01)
Kentucky	The statute is triggered by unauthorized acquisition of unencrypted and unredacted computerized data. (Ky. Rev. Stat. § 365.732)
Louisiana	Notification requirement only applies where the personal information was not encrypted or redacted. (La. Stat. § 51:3073)
Maine	The statute only applies to disclosure of information that is not encrypted. (Me. Rev. Stat. tit. 10, § 1347)
Maryland	Statute applies to the acquisition of both unencrypted information and encrypted information when the security key has been accessed. (Md. Code, Comm. Law § 14-3504)
Massachusetts	No notice 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. (Mass. Gen. Laws ch. 93H, § 1)
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. (Mich. Comp. Laws § 445.72)
Minnesota	A person or business must give notice of a security breach if unencrypted personal information is acquired or encrypted personal information is acquired and the encryption key is also acquired. (Minn. Stat. § 325E.61)
Mississippi	Does not cover encrypted data that has been rendered unreadable. (Miss. Code. § 75-24-29)
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. (Mo. Stat. § 407.1500)

Encryption Safe Harbor	
Montana	The statute applies only to disclosures of unencrypted information. (Mont. Code § 30-14-1704)
Nebraska	Notice is not required if data is encrypted or redacted. Data is not considered encrypted if the security key has been acquired. (Neb. Rev. Stat. § 87-802)
Nevada	If the data is encrypted, notice is not required. (Nev. Rev. Stat. § 603A.220)
New Hampshire	Notification is due if unencrypted data is acquired. Data is not be considered to be encrypted if it is acquired in combination with any required key, security code, access code, or password that would permit access to the encrypted data. (N.H. Rev. Stat. § 359-C:19)
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. 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. (N.J. Stat. § 56:8-161)
New Mexico	Notice is required if the key to the encryption is also obtained. (N.M. HB 15)
New York	When the private information is encrypted and the encryption key has not been acquired, there is no duty to notify. If the encryption key is acquired, notification is required. (N.Y. Gen. Bus. Law § 899-aa)
North Carolina	Notification is required if unencrypted data is acquired or if encrypted data is required and the encryption key is also acquired. (N.C. Gen. Stat. § 75-61)
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. (N.D. Cent. Code § 51-30-01)
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. (Ohio Rev. Code § 1349.19)
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 individual or entity reasonably believes that such breach has caused or will cause identity theft or other fraud to residents. (Okla. Stat. tit. 24, § 163).
Oregon	Notice is not required if data is encrypted or redacted unless the encryption key has been acquired. (Or. Rev. Stat. § 646A.602)
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. (73 Pa. Stat. § 2303)
Rhode Island	If the information is encrypted, notice is not required. Data is not considered encrypted if the security key has been acquired. (11 R.I. Gen. Laws § 11-49.3-3)
South Dakota	No data security laws.

Encryption Safe Harbor	
South Carolina	If data is rendered unusable through encryption, redaction, or other methods, notice to consumers is not required. (S.C. Code § 39-1-90)
Tennessee	Notification requirement applies where personal information was unencrypted or where the information was encrypted but the security key has been acquired. (Tenn. Code § 47-18-2107)
Texas	Notification is required if the encryption key is also acquired. (Tex. Bus. & Com. Code § 521.053)
Utah	If the personal information is encrypted or protected by another method that renders the data unreadable or unusable, notice is not required. (Utah Code § 13-44-102)
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. (Vt. Stat. tit. 9, § 2430)
Virginia	The unauthorized acquisition of encrypted or redacted data, without acquisition of the encryption key, does not trigger the notice requirement under this statute. Notification is required if the key is acquired. (Va. Code § 18.2-186.6)
Washington	Notification is required if the encryption key or other means to decipher encrypted data is acquired by an unauthorized person. (RCW 19.255.010)
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. (W. Va. Code § 46A-2A-102)
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. (Wis. Stat. § 134.98)
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 no notice is required. (Wyo. Stat. § 40-12-501)
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. (D.C. Code § 28-3851)
Puerto Rico	This statute is triggered when the security, confidentially or integrity of data has been compromised. (10 L.P.R.A. § 4051)

Access, Not Acquisition, Triggers Notification Requirements

Gramm-Leach-Bliley Act (GLBA)	When a financial institution becomes aware of an incident of unauthorized access to sensitive customer information, the institution should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused. If the institution determines that misuse of its information about a customer has occurred or is reasonably possible, it should notify the affected customer as soon as possible. (12 C.F.R. § Pt. 30, App. B)
Health Insurance Portability and Accountability Act of 1996 (HIPAA)	Breach means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information. (45 C.F.R. § 164.402)
Connecticut	The 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 (Conn. Gen. Stat. § 36a-701b)
Florida	"Breach of security" or "breach" means unauthorized access of data in electronic form containing personal information. (Fla. Stat. § 501.171)
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. (N.J.S.A. § 56:8-161)
Rhode Island	"Breach of the security of the system" means unauthorized access or acquisition of unencrypted computerized data information that compromises the security, confidentiality, or integrity of personal information maintained by the municipal agency, state agency or person. (11 R.I. Gen. Laws § 11-49.3-3)
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. (10 L.P.R.A. § 4051)

Risk of Harm Analysis and Notification	
Gramm-Leach-Bliley Act (GLBA)	If the institution determines that misuse of its information about a customer has occurred or is reasonably possible, it should notify the affected customer as soon as possible. (12 C.F.R. § Pt. 30, App. B)

Risk of Harm Analysis and Notification	
Health Insurance Portability and Accountability Act of 1996 (HIPAA)	An acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors: (i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification; (ii) The unauthorized person who used the protected health information or to whom the disclosure was made; (iii) Whether the protected health information was actually acquired or viewed; (iv) The extent to which the risk to the protected health information has been mitigated. (45 C.F.R. § 164.402)
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. (Alaska Stat. § 45.48.010)
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. (A.R.S. § 18-545).
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. (Ark. Code § 4-110-105)
California	No ability to perform a risk of harm analysis in the statute other than the inherent determination that no personal information was acquired. (Cal. Civ. Code § 1798.82)
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. (Colo. Rev. Stat. § 6-1-716)
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. (Conn. Gen. Stat. § 36a-701b)
Delaware	Notification is only required if an investigation determines that the misuse of information about a Delaware resident has occurred or is reasonably likely to occur. (Del. Code tit. 6, § 12B-102)
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. (Fla. Stat. § 501.171)
Georgia	No ability to perform a risk of harm analysis in the statute other than the inherent determination that no personal information was acquired. (Ga. Code § 10-1-912)
Hawaii	No ability to perform a risk of harm analysis in the statute other than the inherent determination that no personal information was acquired. (Haw. Rev. Stat. § 487N-2)

Risk of Harm Analysis and Notification	
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. (Idaho Code § 28-51-105)
Illinois	No ability to perform a risk of harm analysis in the statute other than the inherent determination that no personal information was acquired. (815 Ill. Comp. Stat. 530/10)
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. (Ind. Code § 24-4.9-3-1)
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 resulted or will result from the breach. Such a determination must be documented in writing and the documentation must be maintained for five years. (Iowa Code § 715C.2)
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. (Kan. Stat. § 50-7a02)
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. (Ky. Rev. Stat. § 365.732)
Louisiana	Notification is not required if after reasonable investigation the person or business determines that there is no reasonable likelihood of harm to customers. (La. Stat. § 51:3074)
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. (Me. Rev. Stat. tit. 10, § 1348)
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. (Md. Code , Com. Law § 14-3504)

Risk of Harm Analysis and Notification	
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. (Mass. Gen. Laws ch. 93H, § 3)
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. (Mich. Comp. Laws § 445.72)
Minnesota	No ability to perform a risk of harm analysis in the statute other than the inherent determination that no personal information was acquired. (Minn. Stat. § 325E.61)
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. (Miss. Code. § 75-24-29)
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. (Mo. Stat. § 407.1500)
Montana	Notification required if the unauthorized acquisition of computerized data materially compromises the security, confidentiality, or integrity of personal information and causes or is reasonably believed to cause loss or injury to a Montana resident. (Mont. Code § 30-14-1704)
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. (Neb. Rev. Stat. § 87-803)
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. (Nev. Rev. Stat. § 603A.020)
New Hampshire	Notification is not required if it is determined that misuse of the information has not occurred and is not reasonably likely to occur. (N.H. Rev. Stat. § 359-C:20)
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). (N.J. Stat. § 56:8-163)
New Mexico	Notification to affected New Mexico residents is not required if, after an appropriate investigation, the person determines that the security breach does not give rise to a significant risk of identity theft or fraud.(N.M. HB 15)

Risk of Harm Analysis and Notification	
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. (N.Y. Gen. Bus. Law § 899-aa)
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. (N.C. Gen. Stat. § 75-61)
North Dakota	No ability to perform a risk of harm analysis in the statute other than the inherent determination that no personal information was acquired. (N.D. Cent. Code § 51-30-02)
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. (Ohio Rev. Code § 1349.19)
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. (Okla. Stat. tit. 24, § 163)
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. (Or. Rev. Stat. § 646A.604)
Pennsylvania	Notification required only if the access and acquisition materially compromises the security or confidentiality of personal information. (73 Pa. Stat. § 2302)
Rhode Island	No ability to perform a risk of harm analysis in the statute other than the inherent determination that no personal information was acquired. (11 R.I. Gen. Laws § 11-49.3-4)
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. (S.C. Code § 39-1-90)
South Dakota	No data security and privacy laws.
Tennessee	Notification required for unauthorized acquisition of unencrypted computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the information holder. (Tenn. Code § 47-18-2107)
Texas	No ability to perform a risk of harm analysis in the statute other than the inherent determination that no personal information was acquired. (Tex. Bus. & Com. Code § 521.053)

Risk of Harm Analysis and Notification	
Utah	Notification required if, after a risk of harm analysis, it is determined that a misuse of personal information for identity theft or fraud purposes has occurred, or is reasonably likely to occur. (Utah Code § 13-44-202)
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. (Vt. Stat. tit. 9, § 2435)
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. (Va. Code § 18.2-186.6)
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. (Wash. Rev. Code § 19.255.010)
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. (W. Va. Code § 46A-2A-102)
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. (Wis. Stat. § 134.98)
Wyoming	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. (Wyo. Stat. § 40-12-502)
District of Columbia	No ability to perform a risk of harm analysis in the statute other than the inherent determination that no personal information was acquired. (D.C. Code § 28-3851)
Puerto Rico	No ability to perform a risk of harm analysis in the statute other than the inherent determination that no personal information was accessed. (10 L.P.R.A. § 4051)

Notifying State Attorney General or Other Governmental Departments	
Gramm-Leach-Bliley Act (GLBA)	The financial institution must notify its primary Federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information. Consistent with the Agencies' Suspicious Activity Report ("SAR") regulations, notifying appropriate law enforcement authorities, in addition to filing a timely SAR in situations involving Federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing. (12 C.F.R. § Pt. 30, App. B)

Notifying State Attorney General or Other Governmental Departments	
Health Insurance Portability and Accountability Act of 1996 (HIPAA)	A covered entity shall, following the discovery of a breach of unsecured protected health information as provided in § 164.404(a)(2), notify the Secretary. (45 C.F.R. § 164.408) Breaches involving more than 500 individuals requires notification to all affected individuals, the media, and annual disclosures on the HHS website. (45 C.F.R. §§ 164.406, 164.408)
California	General Breach Notification Statute: Any person who notifies more than 500 California residents as a result of a single breach must electronically submit a single sample copy of the notification letter to the Attorney General. (Cal. Civ. Code § 1798.82)
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. (Conn. Gen. Stat. § 36a-701b)
Florida	A covered entity shall provide notice to the Florida Department of Legal Affairs 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. (Fla. Stat. § 501.171)
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. ((Haw. Rev. Stat. § 487N-2)
Idaho	If the entity is a public agency, it must notify the Attorney General within 24 hours of discovery. (Idaho Code § 28-51-105)
Indiana	Attorney General must be notified regarding a breach. (Ind. Code § 24-4.9-3-1)
Iowa	For a breach of security requiring notification of 500 or more Iowa residents, 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. (Iowa Code § 715C.2)
Louisiana	Not required to notify the Attorney General.
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. (Me. Rev. Stat. tit. 10, § 1348)
Maryland	The Attorney General must be notified prior to notification of individuals. (Md. Code , Com. Law § 14-3504)
Massachusetts	The Attorney General, Director of Consumer Affairs and Business Regulation, must be notified regarding a breach. (Mass. Gen. Laws ch. 93H, § 3)
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. (Mo. Stat. § 407.1500)
Montana	Any person or business that is required to issue a notification pursuant to this section shall simultaneously submit an electronic copy of the notification and a statement providing the date and method of distribution of the notification to the attorney general's consumer protection office, excluding any information that personally identifies any individual who is entitled to receive notification. (Mont. Code § 30-14-1704)

Notifying State Attorney General or Other Governmental Departments	
Nebraska	If notice of a breach of security of the system is required to a Nebraska resident, the individual or commercial entity shall also, not later than the time when notice is provided to the Nebraska resident, provide notice of the breach of security of the system to the Attorney General. (Neb. Rev. Stat. § 87-803)
New Hampshire	Any person engaged in trade or commerce that is subject to RSA 358-A:3, I shall also notify the regulator which has primary regulatory authority over such trade or commerce. All other persons shall notify the New Hampshire attorney general's office. (N.H. Rev. Stat. § 359-C:20)
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. (N.J. Stat. § 56:8-163)
New Mexico	A person that is required to issue notification of a security breach pursuant to the Data Breach Notification Act to more than one thousand New Mexico residents as a result of a single security breach shall notify the office of the attorney general and major consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. Section 1681a(p), of the security breach in the most expedient time possible, and no later than forty-five calendar days. (N.M. HB 15).
New York	In the event that any New York residents are to be notified, the person or business shall notify the state attorney general, the department of state and the division of state police as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York residents. (N.Y. Gen. Bus. Law § 899-aa)
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. (N.C. Gen. Stat. § 75-65)
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. (N.D. Cent. Code § 51-30-02)
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. (Or. Rev. Stat. § 646A.604)
Rhode Island	In the event that more than five hundred (500) Rhode Island residents are affected by a breach, the Rhode Island Attorney General 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. (11 R.I. Gen. Laws § 11-49.3-4).
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. (S.C. Code § 39-1-90)
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. (Vt. Stat. tit. 9, § 2435)

Notifying State Attorney General or Other Governmental Departments	
Virginia	The Office of the Attorney General must be notified following discovery of a breach of personal information. (Va. Code § 18.2-186.6)
Washington	Any person or business that is required to issue a notification pursuant to this section to more than five hundred Washington 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 attorney general. The person or business shall also provide to the attorney general the number of Washington consumers affected by the breach, or an estimate if the exact number is not known. (Wash. Rev. Code § 19.255.010)
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. (10 L.P.R.A. § 4052)

Notifying Credit Reporting Agencies	
Gramm-Leach-Bliley Act (GLBA)	Financial institutions are encouraged to notify nationwide consumer reporting agencies prior to sending notices to a large number of customers that include contact information for the reporting agencies. (12 C.F.R. § Pt. 30, App. B)
Health Insurance Portability and Accountability Act of 1996 (HIPAA)	Not applicable.
Alaska	If a security breach affects more than 1,000 state residents, the information collector must notify all consumer credit agencies that maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. 1681a(p). (Alaska Stat. § 45.48.040)
Arizona	Not required to notify credit reporting agencies.
Arkansas	Not required to notify credit reporting agencies.
California	Not required to notify credit reporting agencies.
Colorado	If an individual or commercial entity is required to notify more than one thousand Colorado residents of a breach of the security of the system, the individual or commercial entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by 15 U.S.C. sec. 1681a(p), of the anticipated date of the notification to the residents and the approximate number of residents who are to be notified. (Colo. Rev. Stat. § 6-1-716)
Connecticut	Not required to notify credit reporting agencies.
Delaware	Not required to notify credit reporting agencies.

Notifying Credit Reporting Agencies	
Florida	If a covered entity discovers circumstances requiring notice pursuant to this section of more than 1,000 individuals at a single time, the covered entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in the Fair Credit Reporting Act, 15 U.S.C. s. 1681a(p), of the timing, distribution, and content of the notices. (Fla. Stat. § 501.171)
Georgia	In the event that an information broker or data collector discovers circumstances requiring notification pursuant to this Code section of more than 10,000 residents of this state at one time, the information broker or data collector shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nation-wide basis, as defined by 15 U.S.C. Section 1681a, of the timing, distribution, and content of the notices. (Ga. Code § 10-1-912)
Hawaii	If the breach involves over 1000 persons, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. section 1681a(p), must be notified of the timing, content and distribution of the notice. (Haw. Rev. Stat. § 487N-2)
Idaho	Not required to notify credit reporting agencies.
Illinois	If a State agency is required to notify more than 1,000 persons of a breach of security, the State agency shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by 15 U.S.C. Section 1681a(p), of the timing, distribution, and content of the notices. (815 Ill. Comp. Stat. 530/12)
Indiana	A data base owner required to make a disclosure to more than one thousand (1,000) consumers shall also disclose to each consumer reporting agency (as defined in 15 U.S.C. 1681a(p)) information necessary to assist the consumer reporting agency in preventing fraud, including personal information of an Indiana resident affected by the breach of the security of a system. (Ind. Code § 24-4.9-3-1)
Iowa	Not required to notify credit reporting agencies.
Kansas	If more than 1,000 state residents must be notified at one time, the person shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by 15 U.S.C. § 1681a(p), of the timing, distribution and content of the notices. (Kan. Stat. § 50-7a02)
Kentucky	If more than one thousand (1,000) persons must be notified of a breach at one (1) time, the person shall also notify, without unreasonable delay, all consumer reporting agencies and credit bureaus that compile and maintain files on consumers on a nationwide basis, as defined by 15 U.S.C. sec. 1681a, of the timing, distribution, and content of the notices. (Ky. Rev. Stat. § 365.732)
Louisiana	Not required to notify credit reporting agencies.

Notifying Credit Reporting Agencies	
Maine	If a person discovers a breach of the security of the system that requires notification to more than 1,000 persons at a single time, the person shall also notify, without unreasonable delay, consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 United States Code, Section 1681a(p). (Me. Rev. Stat. tit. 10, § 1348)
Maryland	If a business is required to give notice of a breach of the security of a system to 1,000 or more individuals, the business also shall notify, without unreasonable delay, each consumer reporting agency that compiles and maintains files on consumers on a nationwide basis, as defined by 15 U.S.C. § 1681a(p), of the timing, distribution, and content of the notices. (Md. Code , Com. Law § 14-3506)
Massachusetts	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. (Mass. Gen. Laws ch. 93H, § 3)
Michigan	If notification is due to 1,000 Michigan residents, the person or agency must notify each consumer reporting agency that compiles and maintains files on consumers on a nationwide basis, as defined in 15 USC 1681a(p), of the security breach without unreasonable delay. (Mich. Comp. Laws § 445.72)
Minnesota	If notice is due to more than 500 persons at one time, the person shall also notify, within 48 hours, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by United States Code, title 15, section 1681a, of the timing, distribution, and content of the notices. (Minn. Stat. § 325E.61)
Mississippi	Not required to notify credit reporting agencies.
Missouri	In the event a person provides notice to more than one thousand consumers at one time, the person shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. Section 1681a(p), of the timing, distribution, and content of the notice. (Mo. Stat. § 407.1500)
Montana	If a business discloses a security breach to any individual pursuant to this section and gives a notice to the individual that suggests, indicates, or implies to the individual that the individual may obtain a copy of the file on the individual from a consumer credit reporting agency, the business shall coordinate with the consumer reporting agency as to the timing, content, and distribution of the notice to the individual. The coordination may not unreasonably delay the notice to the affected individuals. (Mont. Code § 30-14-1704)
Nebraska	Not required to notify credit reporting agencies.
Nevada	If a data collector determines that notification is required to be given pursuant to the provisions of this section to more than 1,000 persons at any one time, the data collector shall also notify, without unreasonable delay, any consumer reporting agency, as that term is defined in 15 U.S.C. § 1681a(p), that compiles and maintains files on consumers on a nationwide basis, of the time the notification is distributed and the content of the notification. (Nev. Rev. Stat. § 603A.220)

Notifying Credit Reporting Agencies	
New Hampshire	If a person is required to notify more than 1,000 consumers of a breach of security pursuant to this section, the person shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by 15 U.S.C. section 1681a(p), of the anticipated date of the notification to the consumers, the approximate number of consumers who will be notified, and the content of the notice. (N.H. Rev. Stat. § 359-C:20)
New Jersey	In the event that a business or public entity discovers circumstances requiring notification pursuant to this section of more than 1,000 persons at one time, the business or public entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile or maintain files on consumers on a nationwide basis, as defined by subsection (p) of section 603 of the federal "Fair Credit Reporting Act" (15 U.S.C. s. 1681a), of the timing, distribution and content of the notices. (N.J. Stat. § 56:8-163)
New Mexico	Must notify major consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. Section 1681a(p), of the security breach in the most expedient time possible, and no later than forty-five calendar days. (N.M. HB 15)
New York	In the event that more than five thousand New York residents are to be notified at one time, the person or business shall also notify consumer reporting agencies as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York residents. (N.Y. Gen. Bus. Law § 899-aa)
North Carolina	In the event a business provides notice to more than 1,000 persons at one time pursuant to this section, the business shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. § 1681a(p), of the timing, distribution, and content of the notice. (N.C. Gen. Stat. § 75-65)
North Dakota	Not required to notify credit reporting agencies.
Ohio	If a person discovers circumstances that require disclosure under this section to more than one thousand residents of this state involved in a single occurrence of a breach of the security of the system, the person shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution, and content of the disclosure given by the person to the residents of this state. (Ohio Rev. Code § 1349.19)
Oklahoma	Not required to notify credit reporting agencies.
Oregon	If a person discovers a breach of security that affects more than 1,000 consumers, the person shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain reports on consumers on a nationwide basis of the timing, distribution and content of the notice the person gave to affected consumers and shall include in the notice any police report number assigned to the breach of security. A person may not delay notifying affected consumers of a breach of security in order to notify consumer reporting agencies. (Or. Rev. Stat. § 646A.604)

Notifying Credit Reporting Agencies	
Pennsylvania	When an entity provides notification under this act to more than 1,000 persons at one time, the entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in section 603 of the Fair Credit Reporting Act (Public Law 91-508, 15 U.S.C. § 1681a), of the timing, distribution and number of notices. (73 Pa. Stat. § 2305)
Rhode Island	In the event that more than five hundred (500) Rhode Island residents are affected by a breach, 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. (11 R.I. Gen. Laws § 11-49.3-4)
South Carolina	If a business provides notice to more than one thousand persons at a time, all consumer reporting agencies that compile and maintain files on a nationwide basis, as defined in 15 USC Section 1681a(p), of the timing, distribution, and content of the notice. (S.C. Code § 39-1-90)
South Dakota	No data security laws.
Tennessee	In the event that a person discovers circumstances requiring notification pursuant to this section of more than one thousand (1,000) persons at one time, the person shall also notify, without unreasonable delay, all consumer reporting agencies and credit bureaus that compile and maintain files on consumers on a nationwide basis, as defined by 15 U.S.C. § 1681a, of the timing, distribution and content of the notices. (Tenn. Code § 47-18-2107)
Texas	If a person is required by this section to notify at one time more than 10,000 persons of a breach of system security, the person shall also notify each consumer reporting agency, as defined by 15 U.S.C. Section 1681a, that maintains files on consumers on a nationwide basis, of the timing, distribution, and content of the notices. The person shall provide the notice required by this subsection without unreasonable delay. (Tex. Bus. & Com. Code § 521.053)
Utah	Not required to notify credit reporting agencies.
Vermont	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. (Vt. Stat. tit. 9, § 2435)
Virginia	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. (Va. Code § 18.2-186.6)
Washington	Not required to notify credit reporting agencies.

Notifying Credit Reporting Agencies	
West Virginia	If an entity is required to notify more than one thousand persons of a breach of security pursuant to this article, the entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on a nationwide basis, as defined by 15 U.S.C. § 1681a (p), of the timing, distribution and content of the notices. (W. Va. Code § 46A-2A-102)
Wisconsin	If, as the result of a single incident, an entity is required to notify 1,000 or more individuals that personal information pertaining to the individuals has been acquired, the entity shall without unreasonable delay notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 USC 1681a(p), of the timing, distribution, and content of the notices sent to the individuals. (Wis. Stat. § 134.98)
Wyoming	Not required to notify credit reporting agencies.
District of Columbia	If any person or entity is required by subsection (a) or (b) of this section to notify more than 1,000 persons of a breach of security pursuant to this subsection, the person shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by section 603(p) of the Fair Credit Reporting Act (84 Stat. 1128; 15 U.S.C. § 1681a(p)), of the timing, distribution and content of the notices. Nothing in this subsection shall be construed to require the person to provide to the consumer reporting agency the names or other personal identifying information of breach notice recipients. (D.C. Code § 28-3852)

Notification Deadlines (other than general provision that notification must be given in most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement).	
Gramm-Leach-Bliley Act (GLBA)	"As soon as possible" after conducting the necessary investigation. No specific time requirement. (12 C.F.R. § Pt. 30, App. B)
Health Insurance Portability and Accountability Act of 1996 (HIPAA)	Covered entities must disclose the breach within 60 days of discovery. A breach shall be treated as discovered by a covered entity as of the first day on which such breach is known to the covered entity, or, by exercising reasonable diligence would have been known to the covered entity. A covered entity shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the covered entity (determined in accordance with the federal common law of agency). (45 C.F.R. § 164.404)
Georgia	Any person or business that maintains computerized data on behalf of an information broker or data collector that includes personal information of individuals that the person or business does not own shall notify the information broker or data collector of any breach of the security of the system within **24 hours** following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. (Ga. Code § 10-1-912)

Notification Deadlines (other than general provision that notification must be given in most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement).	
Florida	Notice must be provided without unreasonable delay, no later than **30 days** after the determination of a breach, unless covered entity receives **15 additional day** extension from the Florida Department of Legal Affairs. (Fla. Stat. § 501.171)
Idaho	State agency must disclose breach to Attorney General within **24 hours** of such discovery. (Idaho Code § 28-51-105)
Iowa	Person must give written notice to the consumer protection division of the office of the attorney general within **five business days** after giving notice of the breach of security to any consumer. (Iowa Code § 715C.2)
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. (Me. Rev. Stat. tit. 10, § 1348)
Maryland	Individuals must be notified within 45 days after the conclusion of the internal investigation concerning the scope and possible harm of the data breach. (Md. Code , Com. Law § 14-3504)
Minnesota	If more than 500 persons are entitled to notice, consumer credit agencies must be notified of the breach within **48 hours**. (Minn. Stat. § 325E.61)
New Mexico	Notification shall be made in the most expedient time possible, but not later than **forty-five calendar days** following discovery of the security breach, except if notification would impede a criminal investigation or if the person needs additional time to determine the scope of the security breach and restore the integrity, security and confidentiality of the data system. (N.M. HB 15)
Ohio	Notice must be provided in the most expedient time possible but not later than **45 days** following the discovery or notification of the breach in the security of the system, subject to the legitimate needs of law enforcement activities. (Ohio Rev. Code § 1349.19)
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. (11 R.I. Gen. Laws § 11-49.3-4)
Tennessee	The disclosure of the breach shall be made immediately, but no later than forty-five (45) days from the discovery or notification of the breach, unless a longer period of time is required due to the legitimate needs of law enforcement. If applicable, the notification shall be made no later than **forty-five (45) days** after the law enforcement agency determines that it will not compromise the investigation. (Tenn. Code § 47-18-2107)
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. The data collector shall notify the Attorney General or the Department, as applicable, of the date of the security breach and the date of discovery of the breach and shall provide a preliminary description of the breach within **14 business days**, consistent with the legitimate needs of law enforcement agencies, of the data collector's discovery of the security breach or when the data collector provides notice to consumers pursuant to this section, whichever is sooner. (Vt. Stat. tit. 9, § 2435)

Notification Deadlines (other than general provision that notification must be given in most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement).	
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. (Wash. Rev. Code § 19.255.010)
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. (Wis. Stat. § 134.98)
Puerto Rico	Clients must be notified as expeditiously as possible, taking into consideration the need of law enforcement agencies to secure possible crime scenes and evidence as well as the application of measures needed to restore the system's security. Within a non-extendable term of **ten (10) days** after the violation of the system's security has been detected, the parties responsible shall inform the Department, which shall make a public announcement of the fact within twenty-four (24) hours after having received the information. (10 L.P.R.A. § 4052)

Required Content Within Notification	
Gramm-Leach-Bliley Act (GLBA)	a. A recommendation that the customer review account statements and immediately report any suspicious activity to the institution; b. A description of fraud alerts and an explanation of how the customer may place a fraud alert in the customer's consumer reports to put the customer's creditors on notice that the customer may be a victim of fraud; c. A recommendation that the customer periodically obtain credit reports from each nationwide credit reporting agency and have information relating to fraudulent transactions deleted; d. An explanation of how the customer may obtain a credit report free of charge; e. Information about the availability of the FTC's online guidance regarding steps a consumer can take to protect against identity theft. The notice should encourage the customer to report any incidents of identity theft to the FTC, and should provide the FTC's Web site address and toll-free telephone number that customers may use to obtain the identity theft guidance and report suspected incidents of identity theft. (12 C.F.R. § Pt. 30, App. B)

Required Content Within Notification	
Health Insurance Portability and Accountability Act of 1996 (HIPAA)	The notification shall include, to the extent possible: (A) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known; (B) A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved); (C) Any steps individuals should take to protect themselves from potential harm resulting from the breach; (D) A brief description of what the covered entity involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and (E) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address. (2) Plain language requirement. The notification required by paragraph (a) of this section shall be written in plain language. (45 C.F.R. § 164.404)
Alaska	No requirements listed in statute.
Arizona	No requirements listed in statute.
Arkansas	No requirements listed in statute.
California	California provides a sample notification within the statute with robust requirements. (Cal. Civ. Code § 1798.82)
Colorado	No requirements listed in statute.
Connecticut	No requirements listed in statute.
Delaware	No requirements listed in statute.

Required Content Within Notification	
Florida	The written notice to the department must include: 1. A synopsis of the events surrounding the breach at the time notice is provided. 2. The number of individuals in this state who were or potentially have been affected by the breach. 3. Any services related to the breach being offered or scheduled to be offered, without charge, by the covered entity to individuals, and instructions as to how to use such services. 4. A copy of the notice required under subsection (4) or an explanation of the other actions taken pursuant to subsection (4). 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. 6. The covered entity must provide the following information to the department upon its request: (a). A police report, incident report, or computer forensics report. (b). A copy of the policies in place regarding breaches. (c). Steps that have been taken to rectify the breach. 7. A covered entity may provide the department with supplemental information regarding a breach at any time. (Fla. Stat. § 501.171) The notice to an individual with respect to a breach of security shall include, at a minimum: 1. The date, estimated date, or estimated date range of the breach of security. 2. A description of the personal information that was accessed or reasonably believed to have been accessed as a part of the breach of security. 3. Information that the individual can use to contact the covered entity to inquire about the breach of security and the personal information that the covered entity maintained about the individual. (Fla. Stat. § 501.171)
Georgia	No requirements listed in statute.
Hawaii	The notice shall be clear and conspicuous. The notice shall include a description of the following: (1) The incident in general terms; (2) The type of personal information that was subject to the unauthorized access and acquisition; (3) The general acts of the business or government agency to protect the personal information from further unauthorized access; (4) A telephone number that the person may call for further information and assistance, if one exists; and (5) Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports. (Haw. Rev. Stat. § 487N-2)
Idaho	No requirements listed in statute.

Required Content Within Notification	
Illinois	The disclosure notification to an Illinois 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 Federal Trade Commission, and (iii) a statement that the individual can obtain information from these sources about fraud alerts and security freezes. The notification shall not, however, include information concerning the number of Illinois residents affected by the breach. (815 Ill. Comp. Stat. 530/10)
Indiana	No requirements listed in statute.
Iowa	Notice pursuant to this section shall include, at a minimum, all of the following: a. A description of the breach of security. b. The approximate date of the breach of security. c. The type of personal information obtained as a result of the breach of security. d. Contact information for consumer reporting agencies. e. Advice to the consumer to report suspected incidents of identity theft to local law enforcement or the attorney general. (Iowa Code § 715C.2)
Kansas	No requirements listed in statute.
Kentucky	No requirements listed in statute.
Louisiana	No requirements listed in statute.
Maine	Notification to credit 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. No requirements listed in statute for notification to individuals or state regulators. (Me. Rev. Stat. tit. 10, § 1348)
Maryland	The notification required under subsection (b) of this section shall include: (1) To the extent possible, a description of the categories of information that were, or are reasonably believed to have been, acquired by an unauthorized person, including which of the elements of personal information were, or are reasonably believed to have been, acquired; (2) Contact information for the business making the notification, including the business' address, telephone number, and toll-free telephone number if one is maintained; (3) The toll-free telephone numbers and addresses for the major consumer reporting agencies; and (4)(i) The toll-free telephone numbers, addresses, and Web site addresses for: 1. The Federal Trade Commission; and 2. The Office of the Attorney General; and (ii) A statement that an individual can obtain information from these sources about steps the individual can take to avoid identity theft. (Md. Code , Com. Law § 14-3504)

	Required Content Within Notification
Massachusetts	The notice to be provided to the resident shall include, but not be limited to, the 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, provided however, that said notification shall not include the nature of the breach or unauthorized acquisition or use or the number of residents of the commonwealth affected by said breach or unauthorized access or use. (Mass. Gen. Laws ch. 93H, § 3) The notice to be provided to the attorney general and said director, and consumer reporting agencies or state agencies if any, shall include, but not be limited to, the nature of the breach of security or unauthorized acquisition or use, the number of residents of the commonwealth affected by such incident at the time of notification, and any steps the person or agency has taken or plans to take relating to the incident. (Mass. Gen. Laws ch. 93H, § 3)
Michigan	The notice shall: (a) Describe the security breach in general terms. (b) Describe the type of personal information that is the subject of the unauthorized access or use. (c) If applicable, generally describe what the agency or person providing the notice has done to protect data from further security breaches. (d) Include a telephone number where a notice recipient may obtain assistance or additional information. (e) Remind notice recipients of the need to remain vigilant for incidents of fraud and identity theft. A notification to credit reporting agencies shall include the number of notices that the person or agency provided to residents of this state and the timing of those notices. (Mich. Comp. Laws § 445.72)
Minnesota	No requirements listed in statute.
Mississippi	No requirements listed in statute.
Missouri	The notice shall at minimum include a description of the following: (a) The incident in general terms; (b) The type of personal information that was obtained as a result of the breach of security; (c) A telephone number that the affected consumer may call for further information and assistance, if one exists; (d) Contact information for consumer reporting agencies; (e) Advice that directs the affected consumer to remain vigilant by reviewing account statements and monitoring free credit reports. (Mo. Stat. § 407.1500)
Montana	No requirements listed in statute.
Nebraska	No requirements listed in statute.
Nevada	No requirements listed in statute.

Required Content Within Notification	
New Hampshire	Notice under this section shall include at a minimum: (a) A description of the incident in general terms. (b) The approximate date of breach. (c) The type of personal information obtained as a result of the security breach. (d) The telephonic contact information of the person subject to this section. (N.H. Rev. Stat. § 359-C:20)
New Jersey	No requirements listed in statute.
New Mexico	Notification shall contain: A. the name and contact information of the notifying person; B. a list of the types of personal identifying information that are reasonably believed to have been the subject of a security breach, if known; C. the date of the security breach, the estimated date of the breach or the range of dates within which the security breach occurred, if known; D. a general description of the security breach incident; E. the toll-free telephone numbers and addresses of the major consumer reporting agencies; F. advice that directs the recipient to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach; and G. advice that informs the recipient of the notification of the recipient's rights pursuant to the federal Fair Credit Reporting Act. (N.M. HB 15)
New York	Regardless of the method by which notice is provided, such notice shall include contact information for the person or business making the notification and a description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so acquired. (N.Y. Gen. Bus. Law § 899-aa)
North Carolina	The notice shall be clear and conspicuous. The notice shall include all of the following: (1) A description of the incident in general terms. (2) A description of the type of personal information that was subject to the unauthorized access and acquisition. (3) A description of the general acts of the business to protect the personal information from further unauthorized access. (4) A telephone number for the business that the person may call for further information and assistance, if one exists. (5) Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports. (6) The toll-free numbers and addresses for the major consumer reporting agencies. (7) The toll-free numbers, addresses, and Web site addresses for the Federal Trade Commission and the North Carolina Attorney General's Office, along with a statement that the individual can obtain information from these sources about preventing identity theft. (N.C. Gen. Stat. § 75-65)
North Dakota	No requirements listed in statute.
Ohio	No requirements listed in statute.

	Required Content Within Notification
Oklahoma	No requirements listed in statute.
Oregon	Notice under this section must include, at a minimum: (a) A description of the breach of security in general terms; (b) The approximate date of the breach of security; (c) The type of personal information that was subject to the breach of security; (d) Contact information for the person that owned or licensed the personal information that was subject to the breach of security; (e) Contact information for national consumer reporting agencies; and (f) Advice to the consumer to report suspected identity theft to law enforcement, including the Attorney General and the Federal Trade Commission. (Or. Rev. Stat. § 646A.604)
Pennsylvania	No requirements listed in statute.
Rhode Island	The notification to individuals must include the following information to the extent known: 1) A general and brief description of the incident, including how the security breach occurred and the number of affected individuals; (2) The type of information that was subject to the breach; (3) Date of breach, estimated date of breach or the date range within which the breach occurred; (4) Date that the breach was discovered; (5) A clear and concise description of any remediation services offered to affected individuals including toll free numbers and websites to contact: (i) The credit reporting agencies; (ii) Remediation service providers; (iii) The attorney general; and (6) A clear and concise description of: the consumer's ability to file or obtain a police report; how a consumer requests a security freeze and the necessary information to be provided when requesting the security freeze; and that fees may be required to be paid to the consumer reporting agencies. (11 R.I. Gen. Laws § 11-49.3-4)
South Carolina	No requirements listed in statute.
South Dakota	No data security and privacy laws.
Tennessee	When the personal information is actually used to commit fraud, notification is required in compliance with the Fair Credit Reporting Act. (Tenn. Code § 47-18-2109) (12 C.F.R. § Pt. 1022, App. I)
Texas	No requirements listed in statute.
Utah	No requirements listed in statute.

Required Content Within Notification	
Vermont	The notice to a consumer shall be clear and conspicuous. The notice shall include a description of each of the following, if known to the data collector: (A) the incident in general terms; (B) the type of personally identifiable information that was subject to the security breach; (C) the general acts of the data collector to protect the personally identifiable information from further security breach; (D) a telephone number, toll-free if available, that the consumer may call for further information and assistance; (E) advice that directs the consumer to remain vigilant by reviewing account statements and monitoring free credit reports; and (F) the approximate date of the security breach; (Vt. Stat. tit. 9, § 2435)
Virginia	Notice required by this section shall include a description of the following: (1) The incident in general terms; (2) The type of personal information that was subject to the unauthorized access and acquisition; (3) The general acts of the individual or entity to protect the personal information from further unauthorized access; (4) A telephone number that the person may call for further information and assistance, if one exists; and (5) Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports. (Va. Code § 18.2-186.6)
Washington	The notification must include, at a minimum, the following information: (i) The name and contact information of the reporting person or business subject to this section; (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. (Wash. Rev. Code § 19.255.010)
West Virginia	The notice shall include: (1) To the extent possible, a description of the categories of information that were reasonably believed to have been accessed or acquired by an unauthorized person, including social security numbers, driver's licenses or state identification numbers and financial data; (2) A telephone number or website address that the individual may use to contact the entity or the agent of the entity and from whom the individual may learn: (A) What types of information the entity maintained about that individual or about individuals in general; and (B) Whether or not the entity maintained information about that individual. (3) The toll-free contact telephone numbers and addresses for the major credit reporting agencies and information on how to place a fraud alert or security freeze. (W. Va. Code § 46A-2A-102)
Wisconsin	The notice shall indicate that the entity knows of the unauthorized acquisition of personal information pertaining to the subject of the personal information. (Wis. Stat. § 134.98)

Required Content Within Notification	
Wyoming	Notice required under subsection (a) of this section shall be clear and conspicuous and shall include, at a minimum: (i) A toll-free number: (A) That the individual may use to contact the person collecting the data, or his agent; and (B) From which the individual may learn the toll-free contact telephone numbers and addresses for the major credit reporting agencies. (ii) The types of personal identifying information that were or are reasonably believed to have been the subject of the breach; (iii) A general description of the breach incident; (iv) The approximate date of the breach of security, if that information is reasonably possible to determine at the time notice is provided; (v) In general terms, the actions taken by the individual or commercial entity to protect the system containing the personal identifying information from further breaches; (vi) Advice that directs the person to remain vigilant by reviewing account statements and monitoring credit reports; (vii) Whether notification was delayed as a result of a law enforcement investigation, if that information is reasonably possible to determine at the time the notice is provided. (Wyo. Stat. § 40-12-502)
District of Columbia	No requirements listed in statute.
Puerto Rico	The notice of breach of the security of the system shall be submitted in a clear and conspicuous manner and should describe the breach of the security of the system in general terms and the type of sensitive information compromised. The notification shall also include a toll free number and an Internet site for people to use in order to obtain information or assistance. (10 L.P.R.A. § 4053)

Notification Triggered by a Breach of Security in Electronic and/or Paper Records	
Gramm-Leach-Bliley Act (GLBA)	Consumer information means any record about an individual, whether in paper, electronic, or other form, that is a consumer report or is derived from a consumer report and that is maintained or otherwise possessed by or on behalf of the for a business purpose. Consumer information also means a compilation of such records. The term does not include any record that does not identify an individual. (12 C.F.R. § Pt. 30, App. B)
Health Insurance Portability and Accountability Act of 1996 (HIPAA)	Protected health information means individually identifiable health information: (1) Except as provided in paragraph (2) of this definition, that is: (i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium. (45 C.F.R. § 160.103)
Alaska	"Acquisition" includes acquisition by photocopying, facsimile, or other paper-based method (Alaska Stat. § 45.48.090)
Arkansas	Definition of "personal information" is not limited to electronic information. (Ark. Code § 4-110-103)

California	The statute only applies to businesses that own or license computerized data but the definition of "personal information" is not limited to computerized information. (Cal. Civ. Code § 1798.82)
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. (Haw. Rev. Stat. § 487N-2)
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. (Ind. Code § 24-4.9-2-2)
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. (Iowa Code § 715C.1)
Massachusetts	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. (Mass. Gen. Laws ch. 93H, § 1)
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. (N.C. Gen. Stat. § 75-65)
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 . . . (11 R.I. Gen. Laws § 11-49.3-3)
Washington	The statute's definition of "personal information" and "breach of the security system) is not limited to computerized data alone. (*See* Wash. Rev. Code § 19.255.010)
Wisconsin	The statute's definition of "personal information" is not restricted to computerized information alone. (Wis. Stat. §§ 134.97, 134.98)