

DATA BREACH CHARTS

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

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

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

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

- [States In Which Definition for "Personal Information" is Broader Than the General Definition](#)
- [States That Trigger Notification by Access](#)
- [States That Require a Risk of Harm Analysis](#)
- [States That Require Notice to Attorney General or State Agency](#)
- [States That Require Notification Within a Specific Time Frame](#)
- [States That Permit a Private Cause of Action](#)
- [States With an Encryption Safe Harbor](#)
- [States Where the Statute is Triggered By a Breach of Security in Electronic and/or Paper Records](#)

States in Which Definition for "Personal Information" is Broader than the General Definition

Alaska	<u>Personal Information</u> of Alaska residents. In addition: passwords, personal identification numbers, or other access codes for financial accounts.
Arkansas	<u>Personal Information</u> of Arkansas residents. In addition: medical information.
California	<p><u>General Breach Notification Statute:</u> <u>Personal Information</u> 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.</p> <p><u>Medical Information Specific Breach Notification Statute:</u> 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.</p> <p>"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.</p>
Florida	<p><u>Personal Information</u> means either of the following:</p> <p>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.</p> <p>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.</p>
Georgia	<u>Personal Information</u> of Georgia residents. In addition: a password and any of the data elements not in connection with the name if any of the other data elements alone would be sufficient to perform or attempt to perform identity theft against the person whose information was compromised.
Iowa	<u>Personal Information</u> 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.

States in Which Definition for “Personal Information” is Broader than the General Definition

Kansas	<u>Personal Information</u> of Kansas residents. In addition: an account number or credit card/debit card number, <u>alone or in combination with</u> any required security code, access code or password that would permit access to a consumer’s financial account.
Maine	<u>Personal Information</u> 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.
Maryland	<u>Personal Information</u> of Maryland residents. In addition: an individual Taxpayer Identification Number.
Massachusetts	<u>Personal Information</u> of Massachusetts residents. In addition: financial account information <u>with or without</u> password or security code information. This includes non-electronic personal information.
Missouri	<u>Personal Information</u> 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.
Nebraska	<u>Personal Information</u> 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.
New Hampshire	<u>Medical Information Unauthorized Disclosure Notification Statute</u> : For persons, corporations, facilities, or institutions either licensed in New Hampshire or otherwise lawfully providing health care services, the state’s Medical Information Unauthorized Disclosure Notification statute may apply. The statute applies to protected medical information from §§262 and 264 of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (codified at 42 U.S.C. § 300gg and 29 U.S.C § 1181 et seq. and 42 USC 1320d et seq. (2010)).
New Jersey	<u>Personal Information</u> of New Jersey residents. In addition: dissociated data that, if linked, would constitute personal information is personal information if the means to link the dissociated data were accessed in connection with access to the dissociated data.
New 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

States in Which Definition for "Personal Information" is Broader than the General Definition

	<p>financial account.</p> <p>"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.</p> <p>Private information does not include publicly available information which is lawfully made available to the general public from federal, state, or local government records.</p>
<p>North Carolina</p>	<p>A person's first name or initial and last name, in combination with any one or more of the following:</p> <ol style="list-style-type: none"> (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. <p>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.</p>
<p>North Dakota</p>	<p>"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:</p> <ol style="list-style-type: none"> (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; or (10) the individual's digitized or other electronic signature.
<p>Ohio</p>	<p><u>Personal Information</u> 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:</p> <ol style="list-style-type: none"> 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;

States in Which Definition for “Personal Information” is Broader than the General Definition

	4) any type of media similar in nature to any item, entity, or activity identified above.
Oregon	<p>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:</p> <p>(1) Social Security number; driver license number or state identification card number issued by the Department of Transportation;</p> <p>(2) passport number or other United States issued identification number; or</p> <p>(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.</p> <p>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.</p> <p>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.</p>
South Carolina	<p><u>Personal Information</u> 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.</p>
Texas	<p>The statute applies to “Sensitive personal information”, which includes <u>Personal Information</u> of Texas residents. In addition: information that identifies an individual and relates to:</p> <p>1) the physical or mental health or condition of the individual;</p> <p>2) the provision of health care to the individual; or</p> <p>3) payment for the provision of health care to the individual.</p>
Vermont	<p>“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:</p> <p>(i) Social Security number;</p> <p>(ii) motor vehicle operator’s license number or non-driver identification card number;</p> <p>(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;</p> <p>(iv) account passwords or personal identification numbers or other access codes for a financial account.</p>
Virginia	<p><u>Personal Information Breach Notification Statute</u>: <u>Personal Information</u> of Virginia residents. In addition: medical information.</p> <p><u>Medical Information Breach Notification Statute</u>: 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</p>

States in Which Definition for "Personal Information" is Broader than the General Definition

	<p>by public funds, the state's Medical Information Breach Notification statute may apply. The statute applies to Medical information.</p> <p>"Medical information" means the first name or first initial and last name with any of the following elements:</p> <p>(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</p> <p>(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.</p>
Wisconsin	<p>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:</p> <p>(1) the individual's Social Security number;</p> <p>(2) the individual's driver's license number or state identification number;</p> <p>(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;</p> <p>(4) DNA profile;</p> <p>(5) the individual's unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation.</p>
Wyoming	<p>"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:</p> <p>(A) Social Security number;</p> <p>(B) driver's license number or Wyoming identification card number;</p> <p>(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;</p> <p>(D) tribal identification card; or</p> <p>(E) federal or state government issued identification card.</p>
District of Columbia	<p>A person's first name or first initial and last name, or phone number, or address, in combination with one of the following:</p> <p>(1) Social Security number;</p> <p>(2) driver's license number or District of Columbia Identification Card number</p> <p>(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.</p>
Puerto Rico	<p>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:</p> <p>(1) Social Security number;</p> <p>(2) driver's license number, voter's identification or other official identification;</p> <p>(3) bank or financial account numbers of any type with or without passwords or access code that may have been assigned;</p> <p>(4) names of users and passwords or access codes to public or private</p>

States in Which Definition for “Personal Information” is Broader than the General Definition

	<p>information systems; (5) medical information protected by the HIPAA; (6) tax information; (7) work-related evaluations.</p>
--	---

States that Trigger Notification by Access

Connecticut	<p>“Breach of security” means <u>unauthorized access to</u> 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.</p>
New Jersey	<p>“Breach of security” means <u>unauthorized access to</u> 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.</p>
Puerto Rico	<p>“Violation of the system’s security” means <u>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.</u></p>

States That Require a Risk of Harm Analysis in Determining When Notification is Triggered

Alaska	<p>Notice is not required if, after an investigation and written notice to the Attorney General, the entity determines that there is not a <u>reasonable likelihood that harm to the consumers has or will result</u>. The determination must be documented in writing and maintained for five years.</p>
Arizona	<p>Notice is not required if the breach does not <u>materially compromise</u> 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.</p>
Arkansas	<p>Notification under this section is not required if, after a reasonable investigation, the person or business determines that there is <u>no reasonable likelihood of harm to customers</u>.</p>
Colorado	<p>Notification is not required if after a good-faith, prompt and reasonable investigation, the entity determines that <u>misuse of personal information about a Colorado resident has not occurred and is not likely to occur</u>.</p>
Connecticut	<p>Notification is not required if, after a reasonable investigation and consultation with relevant law enforcement agencies, it is determined that there is <u>no reasonable likelihood of harm to customers</u>.</p>

States That Require a Risk of Harm Analysis in Determining When Notification is Triggered

Delaware	Notification is only required if an investigation determines that the <u>misuse of information</u> about a Delaware resident <u>has occurred</u> or is reasonably likely to occur.
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 <u>has not and will not likely result in identity theft or any other financial harm to the individuals whose personal information has been accessed</u> . Such a determination must be documented in writing and maintained for at least 5 years.
Hawaii	Notification is not required if the entity determines after a reasonable investigation that there is <u>no reasonable likelihood of harm</u> .
Idaho	Notification required if the security, confidentiality, or integrity of the personal information for one or more persons is <u>materially compromised</u> and an investigation determines that the <u>misuse of information</u> about an Idaho resident has occurred or is <u>reasonably likely to occur</u> .
Indiana	Notification required if the database owner knows, should know, or should have known that the unauthorized acquisition constituting the breach <u>has resulted in or could result in identity deception, identity theft, or fraud</u> affecting the Indiana resident.
Iowa	Notification is not required if, after an appropriate investigation or after consultation with the relevant federal, state, or local agencies responsible for law enforcement, the person determined that <u>no reasonable likelihood of financial harm</u> 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.
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 <u>misuse of information has occurred or is reasonably likely to occur</u> , the person or government, governmental subdivision or agency shall give notice as soon as possible to the affected Kansas resident.
Kentucky	Notification is required if the unauthorized acquisition of unencrypted and unredacted computerized data that compromises the security, confidentiality, or integrity of personally identifiable information maintained by the information holder as part of a database regarding multiple individuals <u>actually causes or leads the information holder to reasonably believe has caused or will cause identity theft or fraud</u> against any Kentucky resident.
Louisiana	Notification is not required if after reasonable investigation the person or business determines that there is <u>no reasonable likelihood of harm</u> to customers.
Maine	Notification is not required if after conducting a good-faith, reasonable and prompt investigation, the entity determines that there is <u>not a reasonable likelihood that the personal information has been or will be misused</u> .
Maryland	Notification is not required if after a good-faith, reasonable and prompt investigation the entity determines that the personal information of the individual <u>was not and will not be misused as a result of the breach</u> . If after the investigation

States That Require a Risk of Harm Analysis in Determining When Notification is Triggered

	is concluded, the entity determines that notification is not required, the entity shall maintain records that reflect its determination for three years after the determination is made.
Massachusetts	The breach must create a <u>substantial risk of identity theft or fraud</u> against a resident of the commonwealth or when the person or agency knows or has reason to know that the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose.
Michigan	The person or agency does not have to provide notice if the person or agency determines that the security breach <u>has not or is not likely to cause substantial loss or injury to, or result in identity theft</u> with respect to, one or more residents of Michigan. In making this determination, a person or agency shall act with the care an ordinarily prudent person or agency in like position would exercise under similar circumstances.
Mississippi	Notification is not required if, after an appropriate investigation, the person reasonably determines that the breach will <u>not likely result in harm</u> to the affected individuals.
Missouri	Notification is not required if, after an appropriate investigation by the person or after consultation with the relevant federal, state, or local agencies responsible for law enforcement, the person determines that <u>a risk of identity theft or other fraud to any consumer is not reasonably likely to occur</u> as a result of the breach. Such a determination shall be documented in writing and the documentation shall be maintained for five years.
Montana	Notification required if the unauthorized acquisition of computerized data <u>materially compromises</u> the security, confidentiality, or integrity of personal information and causes or is reasonably believed to cause loss or injury to a Montana resident.
Nebraska	If the investigation determines that the use of information about a Nebraska resident for an <u>unauthorized purpose has occurred or is reasonably likely to occur</u> , the individual or commercial entity shall give notice to the affected Nebraska resident.
Nevada	Notification is required if the unauthorized acquisition of computerized data <u>materially compromises</u> the security, confidentiality, or integrity of personal information maintained by the data collector.
New Hampshire	For Personal Information Breach Notification Statute: Notification is not required if it is determined that <u>misuse of the information has not occurred and is not reasonably likely to occur</u> .
New Jersey	Notification is not required if the business or public entity establishes that <u>misuse of the information is not reasonably possible</u> (must retain a record of this decision for five years).
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.

States That Require a Risk of Harm Analysis in Determining When Notification is Triggered

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 <u>no material risk of harm to a consumer</u> .
Ohio	Notification required only if the access and acquisition by the unauthorized person causes or reasonably is believed will cause a <u>material risk of identity theft or other fraud</u> to the resident.
Oklahoma	Notification required if the breach causes, or the individual or entity <u>reasonably believes has caused or will cause, identity theft or other fraud</u> to any resident of this state.
Oregon	For a person that owns the data, notification is not required if, after an appropriate investigation or after consultation with relevant federal, state or local agencies responsible for law enforcement, the person determines that <u>no reasonable likelihood of harm</u> to the consumers whose personal information has been acquired has resulted or will result from the breach. Such a determination must be documented in writing and the documentation must be maintained for five years.
Pennsylvania	Notification required only if the access and acquisition <u>materially compromises</u> the security or confidentiality of personal information.
Rhode Island	Notification of a breach is not required if, after an appropriate investigation or after consultation with relevant federal, state, or local law enforcement agencies, a determination is made that the breach <u>has not and will not likely result in a significant risk of identity theft</u> to the individuals whose personal information has been acquired.
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 <u>reasonably likely to occur or use of the information creates a material risk of harm</u> to the resident.
Tennessee	Notification required for unauthorized acquisition of unencrypted computerized data that <u>materially compromises</u> the security, confidentiality, or integrity of personal information maintained by the information holder.
Utah	Notification required if <u>misuse of personal information for identity theft or fraud purposes</u> has occurred, or is reasonably likely to occur
Vermont	Notice of a security breach is not required if the data collector establishes that <u>misuse of personal information is not reasonably possible</u> and the data collector provides notice of the determination and a detailed explanation for said determination to the Vermont attorney general or to the department of banking, insurance, securities, and health care administration. If the data collector later gathers facts to indicate that the misuse of personal information is reasonably possible, then notice is required.
Virginia	Notification required if the entity reasonably believes that such a breach <u>has caused or will cause identity theft or other fraud</u> to any resident of the Commonwealth.
Washington	A person, business, or agency <u>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 criminal activity</u> .
West Virginia	Notification required only if the individual or entity reasonably believes the breach <u>has caused or will cause identity theft or other fraud</u> to any resident of this State.

States That Require a Risk of Harm Analysis in Determining When Notification is Triggered

Wisconsin	Notification is not required if the acquisition of personal information <u>does not create a material risk of identity theft or fraud</u> to the subject of the personal information.
Wyoming	<p>Notification is required when unauthorized acquisition of computerized data <u>materially compromises</u> 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.</p> <p>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.</p>

States that Require Notice to Attorney General or State Agency

Alaska	If an entity determines after an investigation that the breach does not create a reasonable likelihood that harm to the consumers has or will result, it must document this determination and provide notice of the determination to the Attorney General.
California	<p><u>General Breach Notification Statute</u>: 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.</p> <p><u>Medical Information Specific Breach Notification Statute</u>: The California Department of Health Services must be notified no later than 5 business days after the unauthorized access, use, or disclosure has been detected by the licensee.</p>
Connecticut	<p>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.</p> <p>Pursuant to Bulletin IC-25 (Aug. 18, 2010), all licensees and registrants of the Connecticut Insurance Department are required to notify the Department of any information security incident which affects any Connecticut residents as soon as the incident is identified, but no later than five calendar days after the incident is identified.</p>
Florida	A covered entity shall provide notice to the Florida Attorney General's Office of any breach of security affecting 500 or more Florida residents. Such notice shall be provided as expeditiously as practicable, but no later than 30 days after determination of the breach or reason to believe a breach has occurred.
Hawaii	If the breach involves over 1000 persons, the Hawaii Office of Consumer Protection must be notified of the timing, content and distribution of the notice.
Idaho	<p>If the entity is a public agency, it must notify the Attorney General within 24 hours of discovery.</p> <p>The agency must also report a security breach to the Office of the Chief Information Officer within the Department of Administration, pursuant to the Information Technology Resource Management Council policies.</p>

States that Require Notice to Attorney General or State Agency

Illinois	Any state agency that collects personal information and has had a breach of security of the system data or written material shall submit a report within five business days of the discovery or notification of the breach to the General Assembly listing the breaches and outlining any corrective measures that have been taken to prevent future breaches of the security of the system data or written material. Any agency that has submitted a report under the statute shall submit an annual report listing all breaches of security of the system data or written materials and the corrective measures that have been taken to prevent future breaches.
Indiana	The Attorney General must be notified regarding a breach.
Iowa	For a breach of security requiring notification of 500 or more Iowa residents pursuant to Iowa law, written notification must be provided to the director of the consumer protection division of the Iowa Attorney General within five business days of notifying any Iowa residents regarding the breach. (Effective July 1, 2014)
Louisiana	When notice must be given to Louisiana citizens, the entity must provide written notice detailing the breach of the security of the system to the Consumer Protection Section of the Attorney General's office. Notice shall include names of all Louisiana citizens affected. Notice to the state Attorney General shall be timely if received within 10 days of the distribution of notice to LA citizens. Each day notice is not received by the state Attorney General shall be deemed a separate violation.
Maine	The Attorney General or Department of Professional and Financial Regulation if the entity is governed by that body must be notified regarding a breach.
Maryland	The Attorney General must be notified prior to notification of individuals.
Massachusetts	The Attorney General, Director of Consumer Affairs and Business Regulation, must be notified regarding a breach. Upon receipt of notice, the Director of Consumer Affairs and Business Regulation will identify any relevant Consumer Reporting Agency or state agency that needs to be notified to the notifying party.
Missouri	If 1,000 or more persons are affected, then the Attorney General must be notified regarding the timing, distribution and content of notice to individuals.
New Hampshire	A person engaged in trade or commerce shall notify the regulator which has primary regulatory authority over such trade or commerce. All other persons shall notify the Attorney General's office. Notice to the Attorney General's office must include the anticipated date of the notice to the individuals and the approximate number of individuals in the state who will be notified. The names of the individuals entitled to receive notice do not have to be disclosed.
New Jersey	The Division of State Police in the Law Department of Law and Public Safety must be notified regarding a breach prior to notifying customers.
New York	The Attorney General, Consumer Protection Board, and the state Office of Cyber Security and Critical Infrastructure must be notified regarding a breach via form notice.
North Carolina	The Consumer Protection Division of the Attorney General's Office must be notified of the nature of the breach, the number of consumers affected, steps taken to investigate the breach, steps taken to prevent a similar breach in the future, and information regarding the timing, distribution, and content of the notice via form notice.
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

States that Require Notice to Attorney General or State Agency	
	shall make a public announcement of the fact within 24 hours of receiving information).
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.
Vermont	<p>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.</p> <p>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.</p>
Virginia	<p><u>Personal Information Breach Notification Statute:</u> The Office of the Attorney General must be notified following discovery of a breach of personal information.</p> <p>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.</p> <p><u>Medical Information Breach Notification Statute:</u> The Office of the Attorney General and the Commissioner of Health must be notified following discovery of a breach of medical information. The entity must notify both the subject of the medical information and any affected resident of the Commonwealth, if those are not the same person.</p> <p>In the event an entity provides notice to more than 1,000 persons at one time, they must notify, without unreasonable delay, the Office of the Attorney General and the Commissioner of Health of the timing, distribution, and content of the notice sent to affected individuals.</p>

States that Require Notification within a Specific Time Frame (other than the general provision that notification must be given in the most expedient time and manner possible and without unreasonable delay, consistent with the legitimate needs of law enforcement).	
California	<u>Medical Information Specific Breach Notification Statute:</u> For clinics, health facilities, home health agencies, and hospices licensed pursuant to sections 1204, 1250, 1725, or 1745 of the California Health and Safety Code, the state's Medical Information Breach Notification statute may apply. The statute requires licensees to notify both affected patients and the California Department of Health Services no later than 5 business days after the unauthorized access, use, or disclosure has been detected by the licensee.
Connecticut	Pursuant to Bulletin IC-25 (Aug. 18, 2010), all licensees and registrants of the Connecticut Insurance Department are required to notify the Department of any information security incident which affects any Connecticut residents as soon as the incident is identified, but no later than five calendar days after the incident is identified.

States that Require Notification within a Specific Time Frame (other than the general provision that notification must be given in the most expedient time and manner possible and without unreasonable delay, consistent with the legitimate needs of law enforcement).

Florida	Notice must be provided without unreasonable delay; no later than 30 days; law enforcement can delay notification.
Maine	If, after the completion of an investigation, notification is required under this section, the notification required by this section may be delayed for no longer than 7 business days after a law enforcement agency determines that the notification will not compromise a criminal investigation.
Ohio	Notice must be provided in the most expedient time possible but not later than 45 days following its discovery or notification of the breach in the security of the system, subject to the legitimate needs of law enforcement activities.
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.
Wisconsin	Notice shall be provided within a reasonable time, not to exceed 45 days after the entity learns of the acquisition of personal information. A determination as to reasonableness shall include consideration of the number of notices that an entity must provide and the methods of communication available to the entity.

States That Permit a Private Cause of Action

Alaska	A person injured by a breach may bring an action against a non-governmental agency under the Unfair or Deceptive Act or Practices, AS 45.50.471 – 45.50.561.
California	Any customer injured by a violation of the general breach notification statute may institute a civil action to recover damages. Any business that violates, proposes to violate, or has violated this title may be enjoined.
Louisiana	A civil action may be instituted to recover actual damages resulting from the failure to disclose in a timely manner to a person that there has been a breach of the security system resulting in the disclosure of a person's personal information.
Maryland	Consumers may bring actions under Title 13 of the Maryland Code, the Unfair and Deceptive Trade Practices Act.
Massachusetts	Massachusetts consumers may seek damages under Chapter 93A, which allows for certain instances of treble damages.
Nevada	A private right of action exists for the data collector. A data collector that provides the requisite notice may commence an action for damages against a person that unlawfully obtained or benefited from personal information obtained from records maintained by the data collector.
New Hampshire	<p>Persons injured as a result of a violation may bring an action for damages and for such equitable relief as the court deems necessary and proper. A prevailing plaintiff shall be awarded the costs of the suit and reasonable attorney's fees.</p> <p>An aggrieved individual whose health records were wrongly disclosed may bring a civil action under RSA 332-I:4 or RSA 332-I:5 and, if successful, shall be awarded special or general damages of not less than \$1,000 for each violation, and costs and reasonable legal fees.</p>

States That Permit a Private Cause of Action	
North Carolina	Provides a private right of action only if individual is injured as a result of the violation. Damages set at a maximum of up to \$5,000, per incident, and provides for treble damages within this range. Injunctive relief also available.
Oregon	Compensation can be ordered by the state upon a finding that enforcement of the rights of consumers by private civil action would be so burdensome or expensive as to be impractical.
South Carolina	A resident of SC who is injured by a violation of this section, in addition to and cumulative of all other rights and remedies available at law, may: institute a civil action to recover damages in case of a willful and knowing violation; institute a civil action to recover only actual damages resulting from a violation in case of a negligent violation; seek an injunction to enforce compliance; and recover attorney's fees and court costs, if successful.
Tennessee	A violation under the data breach notification statute may also be a violation of the Tennessee Consumer Protection Act, which could give rise to a private cause of action.
Texas	A violation under the data breach notification statute may also be a violation of the Texas Deceptive Trade Practices Act, which could give rise to a private cause of action.
Virginia	Though generally enforced by the Attorney General, nothing in the data breach notification statute will preclude recovery of economic damages.
Washington	Any customer injured by a violation may institute a civil action to recover damages.
District of Columbia	Any District of Columbia resident injured by a violation may institute a civil action to recover actual damages, the costs of the action, and reasonable attorney's fees. Actual damages shall not include dignitary damages, including pain and suffering.
Puerto Rico	Consumers may bring actions apart from the statute.
Virgin Islands	Any customer injured by a violation may commence a civil action to recover damages.

States With an Encryption Safe Harbor	
Alaska	The statute only applies to unencrypted information or encrypted information when the encryption key has also been disclosed.
Arizona	Notification requirement only applies where personal information was unencrypted.
Arkansas	Statute only applies to unencrypted data elements.
California	Notification under the general breach notification statute only applies where unencrypted personal information was acquired, or is believed to be acquired, by an unauthorized person.
Colorado	Statute applies only to the disclosure of unencrypted computerized data.
Connecticut	A breach of security only occurs when access to the personal information has not been secured by encryption or by any other method or technology that renders personal information unreadable or unusable.
Delaware	The statute applies to unencrypted computerized data.

States With an Encryption Safe Harbor	
Florida	The statute applies to unencrypted information.
Georgia	The statute applies to unencrypted personal information.
Hawaii	The statute applies only to disclosure of unencrypted or unredacted information.
Idaho	The statute applies to unencrypted personal information.
Illinois	The statute applies to not encrypted personal information.
Indiana	The statute does not apply to encrypted information, provided that the unauthorized recipient of the information does not also get an encryption key.
Iowa	The statute does not cover personal information if it is “encrypted, redacted, or otherwise altered in such a manner that the name or data elements are unreadable” unless the keys to unencrypt, unredact, or otherwise read the data have been obtained through a breach of security. (Effective July 1, 2014)
Kansas	The statute is triggered by disclosure of unencrypted or unredacted information.
Kentucky	The statute is triggered by unauthorized acquisition of unencrypted and unredacted computerized data.
Louisiana	Notification requirement only applies where the personal information was not encrypted or redacted.
Maine	The statute only applies to disclosure of information that is not encrypted.
Maryland	The statute only applies to disclosure of personal information that has not been encrypted, redacted, or otherwise protected by another method that renders the information unreadable or unusable.
Massachusetts	No notice is required as long as the data acquired or used is encrypted, and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information has not been acquired.
Michigan	A person or agency does not have to give notice if the resident’s data was encrypted or redacted, and the person gaining unauthorized access did not have the encryption key.
Minnesota	A person or business must give notice of a security breach if personal information is acquired. Personal information does not include encrypted data.
Mississippi	Does not cover encrypted data.
Missouri	Personal information does not include information that is redacted, altered, or truncated such that no more than five digits of a social security number or the last four digits of a driver’s license number, state identification card number, or account number is accessible as part of the personal information.
Montana	The statute applies only to disclosures of unencrypted information.
Nebraska	Notice is not required if data is encrypted or redacted.
Nevada	If the data is encrypted, notice is not required.
New Hampshire	If the data elements are encrypted, notification is not required.
New Jersey	Statute applies to personal information that has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable.

States With an Encryption Safe Harbor	
New York	When the private information is encrypted and the encryption key has not been acquired, there is no duty to notify.
North Carolina	Notification requirement only applies where the personal information acquired is unencrypted and unredacted.
North Dakota	Notification is not required when data has been secured by encryption or by any other method or technology that renders the electronic files, media, or data bases unreadable or unusable.
Ohio	If the data is encrypted, redacted, or altered by any method or technology in such a manner that the data elements are unreadable, notification is not required.
Oklahoma	Notification is not required for encrypted or redacted information unless the encrypted information is accessed and acquired in an unencrypted form or if the security breach involves a person with access to the encryption key and the individual or entity reasonably believes that such breach has caused or will cause identity theft or other fraud to any resident of this state.
Oregon	If data is encrypted or redacted, notice is not required.
Pennsylvania	Notification is not required when encrypted or redacted information is accessed and acquired. Notice is required, however, if encrypted information is accessed and acquired in an unencrypted form, if the security breach is linked to a breach of the security of the encryption or if the security breach involves a person with access to the encryption key.
Rhode Island	If the information is encrypted, notice is not required.
South Carolina	If data is rendered unusable through encryption, redaction, or other methods, notice to consumers is not required.
Tennessee	Notification requirement only applies where personal information was unencrypted.
Texas	"Sensitive personal information" only applies to data items that are not encrypted.
Utah	If the personal information is encrypted or protected by another method that renders the data unreadable or unusable, notice is not required.
Vermont	Data is not considered personal information if both the individual's name and the combined data element (i.e. social security number) are encrypted, redacted, or protected by another method that renders them unreadable or unusable.
Virginia	The unauthorized acquisition of encrypted or redacted data, without access to the encryption key, does not trigger the notice requirement under this statute.
Washington	If both an individual's first name or first initial and last name and accompanying data element (i.e. social security number) are encrypted, notice is not required.
West Virginia	If encrypted or redacted information is accessed and acquired and the person does not have access to the encryption key, notice is not required.
Wisconsin	If one of the data elements linked to an individual's name is encrypted, redacted, or altered in a manner that renders the element unreadable, it is not considered personal information, meaning no notice is required.
Wyoming	If both an individual's first name or first initial and last name and combined data element (i.e. social security number) are redacted, the data is not considered personal identifying information, and notice is not required.
District of	The acquisition of data that has been rendered secure, so as to be unusable by an

States With an Encryption Safe Harbor	
Columbia	unauthorized third party is not considered a breach of the security system.
Guam	Notification requirement does not apply to encrypted data unless the security breach involves a person with access to the encryption key and the individual or entity reasonably believes that such breach has caused or will cause identity theft or other fraud to any resident of Guam.
Puerto Rico	This statute is triggered only when unencrypted information is disclosed.
Virgin Islands	Statute applies only where personal information was unencrypted.

States Where the Statute is Triggered by a Breach of Security in Electronic and/or Paper Records	
Alaska	“Breach of security” means unauthorized acquisition, or reasonable belief of unauthorized acquisition, or personal information that compromises the security, confidentiality, or integrity of the personal information maintained by the information collector. “Acquisition” includes: acquisition by photocopying, facsimile, <u>or other paper-based method</u> ; a device including a computer, that can read, write or store information that is represented in numerical form; or a method not identified by this paragraph.
Hawaii	This statute applies to any business that owns or licenses personal information of residents of Hawaii, any business that conducts business in Hawaii that owns or licenses personal information in any form (<u>whether computerized, paper, or otherwise</u>), or any government agency that collects personal information for specific government purposes.
Indiana	Breach of the security of data means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person. The term includes the unauthorized acquisition of computerized data that have been transferred to <u>another medium, including paper, microfilm, or a similar medium, even if the transferred data are no longer in a computerized format.</u>
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 <u>maintained by a person in any medium, including on paper</u> , that was transferred by the person to that medium from computerized form and that compromises the security, confidentiality, or integrity of the personal information. (Effective July 1, 2014)
Massachusetts	Breach of security is the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the commonwealth. <u>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.</u>
North Carolina	Statute applies to any business that owns or licenses personal information <u>in any</u>

**States Where the Statute is Triggered by a Breach of Security
in Electronic and/or Paper Records**

	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.
Wisconsin	This statute does not define a “breach of security”, and its definition of “personal information” is not restricted to computerized information alone.

Baker & Hostetler LLP publications are intended to inform our clients and other friends of the Firm about current legal developments of general interest. They should not be construed as legal advice, and readers should not act upon the information contained in these publications without professional counsel. The hiring of a lawyer is an important decision that should not be based solely upon advertisements. Before you decide, [ask us](#) to send you written information about our qualifications and experience. © 2014 Baker & Hostetler LLP