US State Breach Notification Chart

State	Breach notification statute	Notification trigger	Notification time frame (individuals)	Notification to the state attorney general	Notification time frame (state attorney general)	Notification to other government agencies or consumer reporting agencies	Notification time frame (other government agencies or CRAs)	Additional features
Alabama	Ala. Code §§ 8-38-1 to 8-38-12	When a covered entity determines under Ala. Code § 8-38-4 that, as a result of a breach of security, sensitive personally identifying information has been acquired or is reasonably believed to have been acquired by an unauthorized person, and is reasonably likely to cause substantial harm to the individuals to whom the information relates	Notice must be provided as expeditiously as possible and without unreasonable delay, taking into account the time necessary to allow the covered entity to conduct an investigation, but within 45 days of the covered entity's receipt of notice from a third-party agent that a breach has occurred or upon the covered entity's determination that a breach has occurred and is reasonably likely to cause substantial harm, except upon written request of law enforcement as outlined in Ala. Code § 8-38-5(c).	Yes, if notice is required to more than 1,000 individuals	As expeditiously as possible and without unreasonable delay, but within 45 days except upon written request of law enforcement as outlined in Ala. Code § 8-38-5(c)	Yes, to consumer reporting agencies, if notice is required to more than 1,000 individuals	Not specified	
Alaska	Alaska Stat. §§ 45.48.010 et seq.	Notice is required if a breach of the security of an information system that contains personal information of an Alaska resident occurs unless, after an appropriate investigation and after written notification to the attorney general, the covered person determines that there is not a reasonable likelihood of harm to the consumers whose personal information has been acquired.	Notice is required in the most expeditious time possible and without unreasonable delay except upon the determination of law enforcement as outlined in Alaska Stat. § 45.48.020 and as necessary to determine the scope of the breach and restore the reasonable integrity of the information system.	Notice to the attorney general is only required if the covered person intends to invoke the exception from disclosure based on determining that there is not a reasonable likelihood of harm from the breach.	Not specified	Yes, to consumer reporting agencies, if notice to more than 1,000 residents is required	Without unreasonable delay	 (See Alaska Stat. § 45.48.080.)   

 Private right of action

 An individual or entity that maintains personal data that the individual or entity does not own or license (a vendor or other third party) that experiences a breach must notify the owner or licensor of the information.

 Notice not required if data was encrypted and the decryption key was not compromised

 Waiver of statutory provision void and unenforceable

State	Breach notification statute	Notification trigger	Notification time frame (individuals)	Notification to the state attorney general	Notification time frame (state attorney general)	Notification to other government agencies or consumer reporting agencies	Notification time frame (other government agencies or CRAs)	Additional features
Arizona	Ariz. Rev. Stat. §§ 18-551 to 18-552	Notice is required when an investigation conducted by a business that owns, maintains or licenses unencrypted and unredacted computerized personal information determines that a security system breach (defined as an unauthorized acquisition of and unauthorized access that materially compromises the security or confidentiality of unencrypted and unredacted personal information) has occurred, unless it has been determined that the breach has not resulted in or is not reasonably likely to result in substantial economic loss to affected individuals.	Notice must be provided within 45 days except if a law enforcement agency advises that the notifications will impede a criminal investigation, as outlined in Ariz. Rev. Stat. § 18-552.	Yes, to both the state attorney general and the director of the Arizona department of homeland security, if the breach requires notification to more than 1,000 individuals	Within 45 days after a determination that there has been a security system breach	Yes, to the three largest nationwide consumer reporting agencies if the breach requires notification to more than 1,000 individuals	Within 45 days after a determination that there has been a security system breach	
Arkansas	Ark. Code Ann. §§ 4-110-101 to 108	Following discovery or notification of a breach of the security of a system of computerized data where the unencrypted personal information of a resident of Arkansas was, or is reasonably believed to have been, acquired by an unauthorized person, unless, after a reasonable investigation, the person or business determines that there is no reasonable likelihood of harm to customers	Notice must be provided in the most expedient time and manner possible and without unreasonable delay, consistent with the legitimate needs of law enforcement as outlined in Ark. Code Ann. § 4-110-105(c) or any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system.	Yes, notice to the state attorney general is required if the breach affects more than 1,000 individuals.	At the same time the security breach is disclosed to an affected individual or within 45 days after the person or business determines that there is a reasonable likelihood of harm to customers, whichever occurs first	Not required	Not applicable	

Private right of action

An individual or entity that maintains personal data that the individual or entity does not own or license (a vendor or other third party) that experiences a breach must notify the owner or licensor of the information.

Notice not required if data was encrypted and the decryption key was not compromised

Waiver of statutory provision void and unenforceable

State	Breach notification statute	Notification trigger	Notification time frame (individuals)	Notification to the state attorney general	Notification time frame (state attorney general)	Notification to other government agencies or consumer reporting agencies	Notification time frame (other government agencies or CRAs)	Additional features
California	Cal. Civ. Code §§ 1798.80 et seq.; Cal. Health & Safety Code, § 1280.15; 22 Cal. Code Regs. § 79902	An individual 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, or whose encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person and the person or business that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that personal information readable or usable. Additionally, under Cal. Health & Safety Code § 1280.15, a clinic, health facility, home health agency or hospice licensed under state law must report any unlawful or unauthorized access to, or use or disclosure of, a patient's medical information to the affected patient or the patient's representative.	Notice must be provided in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as outlined in Cal. Civ. Code § 1798.82(c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. Effective 1 Jan. 2026, the disclosure must be made within 30 calendar days of discovery or notification of the data breach. For health care facilities providing notice of a breach of medical information required by Cal. Health & Safety Code § 1280.15, notice is required no later than 15 business days after the breach has been detected by the health care facility.	Yes, if notice is required to more than 500 California residents as a result of a single breach	Effective 1 Jan. 2026, the submission to the attorney general must be made within 15 days of notifying affected consumers.	Yes, notification to the California Department of Public Health is required in the case of medical information covered under Cal. Health & Safety Code § 1280.15	No later than 15 business days after the incident is detected, unless the law enforcement agency provides a statement that compliance would likely impede investigation of the incident and specifies a date upon which the delay shall end, not to exceed 60 days after a written request, or 30 days after an oral request, subject to extension	

Private right of action

An individual or entity that maintains personal data that the individual or entity does not own or license (a vendor or other third party) that experiences a breach must notify the owner or licensor of the information.

Notice not required if data was encrypted and the decryption key was not compromised

Waiver of statutory provision void and unenforceable

State	Breach notification statute	Notification trigger	Notification time frame (individuals)	Notification to the state attorney general	Notification time frame (state attorney general)	Notification to other government agencies or consumer reporting agencies	Notification time frame (other government agencies or CRAs)	Additional features
Colorado	Colo. Rev. Stat. § 6-1-716	Upon awareness that a security breach may have occurred, unless a good faith, prompt investigation determines that the misuse of information about a Colorado resident has not occurred and is not reasonably likely to occur	Notice is required in the most expedient time possible and without unreasonable delay, but not later than 30 days after the date of determination that a security breach occurred, consistent with the legitimate needs of law enforcement as outlined in Colo. Rev. Stat. § 6-1-716(c) and any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.	Yes, if the security breach is reasonably believed to have affected 500 Colorado residents or more, unless the investigation determines that the misuse of information about a Colorado resident has not occurred and is not likely to occur	In the most expedient time possible and without unreasonable delay, but not later than 30 days after the date of a determination that a security breach occurred	Yes, to all consumer reporting agencies, if a covered entity is required to notify more than 1,000 Colorado residents	In the most expedient time possible and without unreasonable delay	
Connecticut	Conn. Gen. Stat. § 36a-701b	Notice is required upon the discovery of a breach of security where the personal information of a Connecticut resident was breached or is reasonably believed to have been breached unless an appropriate investigation reasonably determines that the breach will not likely result in harm to the individuals whose personal information has been acquired or accessed.	Notice is required without unreasonable delay but no later than 60 days after the discovery of such breach unless a shorter timeframe is required under federal law or if delay is requested by law enforcement as outlined in Conn. Gen. Stat. § 36a-701b(d).	Yes, notice to the state attorney general is required regardless of the number of persons affected.	No later than time of notification to residents	Not required	Not applicable	
Delaware	Del. Code Ann. tit. 6, § 12B-100 et seq.	Notice is required following the determination of a breach of security where the personal information of a resident of Delaware was breached or is reasonably believed to have been breached, unless after an appropriate investigation the business reasonably determines that the breach is unlikely to result in harm to the individuals whose personal information has been breached.	Notice is required without unreasonable delay, but not later than 60 days after determination of the breach, unless one of the exceptions, which include law enforcement requests, in Del. Code Ann. tit. 6, § 12B-102(c) applies.	Yes, notice to the state attorney general is required if the affected number of Delaware residents to be notified exceeds 500.	No later than notification to residents	Not required	Not applicable	

Private right of action

An individual or entity that maintains personal data that the individual or entity does not own or license (a vendor or other third party) that experiences a breach must notify the owner or licensor of the information.

Notice not required if data was encrypted and the decryption key was not compromised

Waiver of statutory provision void and unenforceable

State	Breach notification statute	Notification trigger	Notification time frame (individuals)	Notification to the state attorney general	Notification time frame (state attorney general)	Notification to other government agencies or consumer reporting agencies	Notification time frame (other government agencies or CRAs)	Additional features
Florida	Fla. Stat. Ann. § 501.171	Notice is required when the personal information of an individual in Florida was, or a covered entity reasonably believes, has been accessed as a result of a breach, unless, 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.	Notice must be provided as expeditiously as practicable and without reasonable delay, taking into account the time necessary to allow the covered entity to determine the scope of the breach of security, to identify individuals affected by the breach, and to restore the reasonable integrity of the data system that was breached, but no more than 30 days after the determination of a breach or reason to believe a breach occurred unless subject to a delay under Fla. Stat. Ann. § 501.171(4)(b) or a waiver under Fla. Stat. Ann. § 501.171(c) (if, after an appropriate investigation and consultation with law enforcement, the covered entity reasonably determines that the breach has not and will not likely result in identity theft or any other financial harm). A covered entity may receive 15 additional days, under requirements outlined in Fla. Stat. Ann. § 501.171(3)(a).	Yes, to state department of legal affairs if 500 or more individuals are affected	As expeditiously as possible, but no more than 30 days after the determination of the breach or reason to believe a breach occurred	Yes, notification to all consumer reporting agencies is mandatory if notice is required to more than 1,000 individuals at a single time.	Without unreasonable delay	
Georgia	Ga. Code Ann. §§ 10-1-910 to 915	Notice is required upon discovery or notification of a breach in the security of a system that contains computerized data; notification is required to any resident of Georgia whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.	Notice must be provided in the most expedient time possible and without unreasonable delay, consistent with the needs of law enforcement as provided in Ga. Code Ann. § 10-1-912(c) or with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security and confidentiality of the data system.	Not required	Not applicable	Yes, notification to all consumer reporting agencies is mandatory if notice is required to more than 10,000 residents at one time.	Without reasonable delay	

 Private right of action

 An individual or entity that maintains personal data that the individual or entity does not own or license (a vendor or other third party) that experiences a breach must notify the owner or licensor of the information.

 Notice not required if data was encrypted and the decryption key was not compromised

 Waiver of statutory provision void and unenforceable

State	Breach notification statute	Notification trigger	Notification time frame (individuals)	Notification to the state attorney general	Notification time frame (state attorney general)	Notification to other government agencies or consumer reporting agencies	Notification time frame (other government agencies or CRAs)	Additional features
Hawaii	Haw. Rev. Stat. § 487N-1 et seq.	Notice is required upon discovery or notification of a security breach. The law's scope includes any business that conducts business in Hawaii that owns or licenses personal information (defined in Haw. Rev. Stat. § 487N-1) in any form (whether computerized, paper or otherwise). Haw. Rev. Stat. § 487N-1 defines security breach as "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."	Notice must be provided without unreasonable delay consistent with the legitimate needs of law enforcement as provided in Haw. Rev. Stat. § 487N-2(c), and consistent with any measures necessary to determine sufficient contact information, determine the scope of the breach, and restore the reasonable integrity, security and confidentiality of the data system.	Not required	Not applicable	Yes, notification to the State of Hawaii's office of consumer protection and all consumer reporting agencies is required if a business provides notice to more than 1,000 persons.	Without reasonable delay	
Idaho	Idaho Code § 28-51-103 to -107	Notification is required when a reasonable and prompt investigation, which an entity conducting business in Idaho and owning or licensing computerized data that includes personal information about a resident of Idaho must conduct in good faith when it becomes aware of a breach of the security of the system, determines that the misuse of information about an Idaho resident has occurred or is reasonably likely to occur.	Notice must be provided as soon as possible, in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement as outlined in Idaho Code § 28-51-105(3) and any measures necessary to determine the scope of the breach, to identify the individuals affected, and to restore the reasonable integrity of the computerized data system.	Yes, notice to the state attorney general is required if the breach occurs within a state agency.	Within 24 hours of discovery if breach occurs in a state agency	Not required	Not applicable	

Private right of action

An individual or entity that maintains personal data that the individual or entity does not own or license (a vendor or other third party) that experiences a breach must notify the owner or licensor of the information.

Notice not required if data was encrypted and the decryption key was not compromised

Waiver of statutory provision void and unenforceable

State	Breach notification statute	Notification trigger	Notification time frame (individuals)	Notification to the state attorney general	Notification time frame (state attorney general)	Notification to other government agencies or consumer reporting agencies	Notification time frame (other government agencies or CRAs)	Additional features
Illinois	815 Ill. Comp. Stat. § 530/1 et seq.	Notice is required following discovery or notification of a breach of personal information (as defined in 815 ILCS 530/5) concerning an Illinois resident. A breach is defined as "the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the data collector."	Notice must be provided in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security and confidentiality of the data system. Notification may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the data collector with a written request.	Yes. Any data collector that is not a state agency is required to notify the state attorney general if it is required to issue notice to more than 500 Illinois residents as a result of a single breach. Any state agency that suffers a single breach of the security of the data concerning the personal information of more than 250 Illinois residents must also notify the attorney general. Any entity required to provide notification of a breach to the federal Secretary of Health and Human Services shall also provide such notification to the state attorney general within five business days of notifying HHS.	Data collector that is not a state agency: in the most expedient time possible and without unreasonable delay, but no later than the notice to consumers. State agency: within 45 days of the agency's discovery of the breach or when the agency provides any required notice to consumers, whichever is sooner, but no later than 72 hours following the discovery of the incident if the agency is directly responsible to the governor.	If a state agency is required to notify more than 1,000 persons of a breach, the agency shall also notify all consumer reporting agencies.	Without unreasonable delay	
Indiana	Ind. Code §§ 24-4.9-1-1 et seq.	Notice is required after discovery or being notified of a breach of the security of data where an Indiana resident's personal information (defined in IC 24-4.9-2-10) was or may have been acquired by an unauthorized person, 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.	Notice must be provided without unreasonable delay, but not more than 45 days after the discovery of the breach, where reasonable delay is defined by IC 24-4.9-3-3(a)(1-3) as a delay necessary to restore the integrity of the computer system or to discover the scope of the breach or in response to a request from the attorney general or a law enforcement agency.	Yes, notice to the state attorney general is required without regard to the number of persons affected.	Without unreasonable delay	Yes, notification to each consumer reporting agency is mandatory if notification is required to more than 1,000 consumers.	Not specified	

Private right of action

An individual or entity that maintains personal data that the individual or entity does not own or license (a vendor or other third party) that experiences a breach must notify the owner or licensor of the information.

Notice not required if data was encrypted and the decryption key was not compromised

Waiver of statutory provision void and unenforceable

State	Breach notification statute	Notification trigger	Notification time frame (individuals)	Notification to the state attorney general	Notification time frame (state attorney general)	Notification to other government agencies or consumer reporting agencies	Notification time frame (other government agencies or CRAs)	Additional features
Iowa	Iowa Code §§ 715C.1 to .2	Notice is required upon the discovery or receipt of notification of a breach of security of the personal information (defined in Iowa Code § 715C.1) of an individual who is a resident of the state. However, notice is not required if, after an appropriate investigation or consultation with the relevant federal, state or local agencies responsible for law enforcement, the covered 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.	Notice must be provided in the most expeditious manner as possible and without unreasonable delay, consistent with the legitimate needs of law enforcement as provided in Iowa Code § 715C.2(3) and with any measures necessary to sufficiently determine contact information for the affected consumers, determine the scope of the breach and restore the reasonable integrity, security and confidentiality of the data.	Yes, to the director of the consumer protection division of the office of the attorney general if notification is required to more than 500 Iowa residents	Within five business days after giving notice to any consumer	Not required	Not applicable	
Kansas	Kan. Stat. Ann. § 50-7a01 et seq.	Notice is required when a reasonable and prompt investigation, which a person conducting business in Kansas or a government agency owning or licensing computerized data that includes personal information (as defined in K.S.A. § 50-7a01) about a resident of Kansas must conduct in good faith when it becomes aware of a breach of the security of the system, determines that the misuse of information has occurred or is reasonably likely to occur.	Notice must be provided as expeditiously as possible and without unreasonable delay, consistent with the legitimate needs of law enforcement as outlined in K.S.A. § 50-7a02(c) and with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.	Not required	Not applicable	Yes, notification to all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis is mandatory if circumstances require notice to more than 1,000 Kansas residents at one time.	Without unreasonable delay	
Kentucky	Ky. Rev. Stat. § 365.732	Notice is required following the discovery or notification of a breach in the security of data where the unencrypted personal information (defined in Ky. Rev. Stat. § 365.732) of any resident of Kentucky was, or is reasonably believed to have been, acquired by an unauthorized person and such breach actually causes, or leads the information holder to reasonably believe has caused or will cause identity theft or fraud against any resident of Kentucky.	Notice must be provided in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as outlined in Ky. Rev. Stat. § 365.732(4), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.	Not required	Not applicable	Yes, notification to all consumer reporting agencies and credit bureaus that compile and maintain files on consumers on a nationwide basis is mandatory if the circumstances require notice to more than 1,000 persons at one time.	Without unreasonable delay	

Private right of action

An individual or entity that maintains personal data that the individual or entity does not own or license (a vendor or other third party) that experiences a breach must notify the owner or licensor of the information.

Notice not required if data was encrypted and the decryption key was not compromised

Waiver of statutory provision void and unenforceable

State	Breach notification statute	Notification trigger	Notification time frame (individuals)	Notification to the state attorney general	Notification time frame (state attorney general)	Notification to other government agencies or consumer reporting agencies	Notification time frame (other government agencies or CRAs)	Additional features
Louisiana	La. Rev. Stat. §§ 51:3071 et seq.; see also La. Admin. Code tit. 16, § 701	Notice is required following discovery of a breach in the security of a system where the personal information (as defined in La. Rev. Stat. § 51-3073) of a resident of Louisiana was, or is reasonably believed to have been, acquired by an unauthorized person. A breach is defined as "the compromise of the security, confidentiality, or integrity of computerized data that results in, or there is a reasonable likelihood to result in, the unauthorized acquisition of and access to personal information." Notice is not required if, after a reasonable investigation, the person or business determines that there is no reasonable likelihood of harm to the residents of the state.	Notice must be provided in the most expeditious time possible and without unreasonable delay but no more than 60 days from discovery of the breach, consistent with the legitimate needs of law enforcement, as provided in La. Rev. Stat. § 51:3074(F), or any measures necessary to determine the scope of the breach, prevent further disclosures, and restore the reasonable integrity of the data system. When the notification is delayed, the person or agency must provide the attorney general the reasons for the delay in writing within the 60-day notification period upon receipt of which the attorney general shall allow a reasonable extension of time to provide the required notification.	Yes, to the Consumer Protection Section of the attorney general's office, if any citizen of Louisiana must be notified (La. Admin. Code tit. 16, Part III, § 701)	Within 10 days of notice to the citizen	Not required	Not applicable	
Maine	10 Me. Rev. Stat. §§ 1346 et seq.	Information brokers maintaining computerized data that includes personal information (as defined in 10 Me. Rev. Stat. § 1347), are required to provide notice following discovery or notification of a breach where the personal information of a resident of the state has been, or is reasonably believed to have been, acquired by an unauthorized person. Information brokers must conduct a reasonable and prompt investigation in good faith to determine the likelihood that personal information has been or will be misused, but the outcome of that investigation is not the trigger. Other persons who maintain computerized data that includes personal information must conduct a reasonable and prompt investigation following the awareness of a breach; notice must be given following the discovery or notification of the security breach if misuse of the personal information of a Maine resident has occurred or if it is reasonably possible that misuse will occur.	Notice must be provided as expediently as possible and without unreasonable delay, consistent with the legitimate needs of law enforcement as outlined in 10 Me. Rev. Stat. § 1348(3) or with measures necessary to determine the scope of the breach and restore the reasonable integrity, security and confidentiality of the data. If there is no delay due to a law enforcement investigation, the notices must be made no more than 30 days after the covered person becomes aware of the breach and identifies its scope.	Yes, if the person is not regulated by the Department of Professional and Financial Regulation	Not specified	Yes, notification to the appropriate state regulators within the Department of Professional and Financial Regulation is required if the covered person is regulated by the department. Notification to consumer reporting agencies is also mandatory if the breach requires notification to more than 1,000 individuals at a single time.	Not specified for notice to the appropriate state regulators within the Department of Professional and Financial Regulation. Without unreasonable delay to the consumer reporting agencies.	

Private right of action

An individual or entity that maintains personal data that the individual or entity does not own or license (a vendor or other third party) that experiences a breach must notify the owner or licensor of the information.

Notice not required if data was encrypted and the decryption key was not compromised

Waiver of statutory provision void and unenforceable

State	Breach notification statute	Notification trigger	Notification time frame (individuals)	Notification to the state attorney general	Notification time frame (state attorney general)	Notification to other government agencies or consumer reporting agencies	Notification time frame (other government agencies or CRAs)	Additional features
Maryland	Md. Code Ann. Com. Law §§ 14-3504 et seq.	Notice is required following the discovery or notification of a breach of the security of a system containing computerized data of an individual residing in Maryland, unless the business reasonably determines after a reasonable and prompt investigation that the breach does not create a likelihood that personal information (as defined in Md. Code Ann. Com. Law § 14-3501) has been or will be misused.	Notice must be provided as soon as reasonably practicable but no later than 45 days after the business discovers or is notified of the breach except upon a law enforcement determination as outlined by Md. Code Ann. Com. Law § 14-3504(d), or to determine the scope of the breach, identify the individuals affected, or restore the integrity of the system	Yes	Prior to notification to impacted individuals	Yes, if notification is required to 1,000 or more individuals	Without unreasonable delay	
Massachusetts	Mass. Gen. Laws ch. 93H, §§ 1 et seq.	Notice is required when a person or agency that owns or licenses data that includes personal information (as defined in Mass. Gen. Laws ch. 93H, § 1) about a resident of Massachusetts either: (1) knows or has reason to know of a breach of security; or (2) knows or has reason to know that the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose.	Notice must be provided as soon as practicable and without unreasonable delay, except upon the determination of law enforcement as outlined in Mass. Gen. Laws ch. 93H, § 4. Notice shall not be delayed on grounds that the total number of residents affected is not yet ascertained. In such case and where it is otherwise necessary to update or correct the information required, a person or agency shall provide additional notice as soon as practicable and without unreasonable delay upon learning such additional information.	Yes	As soon as practicable and without unreasonable delay	Yes, notification to the director of consumer affairs and business regulation and to any relevant consumer reporting agencies and state agencies identified by the director is required.	As soon as practicable and without unreasonable delay	* *See definition of "breach of security" and compare with breach trigger for acquisition by unauthorized person.

Private right of action

An individual or entity that maintains personal data that the individual or entity does not own or license (a vendor or other third party) that experiences a breach must notify the owner or licensor of the information.

Notice not required if data was encrypted and the decryption key was not compromised

Waiver of statutory provision void and unenforceable

State	Breach notification statute	Notification trigger	Notification time frame (individuals)	Notification to the state attorney general	Notification time frame (state attorney general)	Notification to other government agencies or consumer reporting agencies	Notification time frame (other government agencies or CRAs)	Additional features
Michigan	Mich. Comp. Laws §§ 445.63, 445.72	Notice is required upon the discovery or notification of a security breach where either a Michigan resident's unencrypted and unredacted personal information (as defined in Mich. Comp. Laws § 445.63) was accessed and acquired by an unauthorized person or a resident's personal information was accessed and acquired in encrypted form by a person with unauthorized access to the encryption key. Notice is not required if the person or agency determines that the breach has not or is not likely to cause substantial loss or injury to, or result in identify theft with respect to, one or more residents of the state.	Notice must be provided without unreasonable delay, except where a delay is necessary for the person or agency to take any measures necessary to determine the scope of the security breach and restore the reasonable integrity of the database or where a law enforcement agency determines that notice would impede a criminal or civil investigation, as outlined in Mich. Comp. Laws § 445.72(4)(b).	Not required	Not applicable	Yes, notification to consumer reporting agencies is mandatory if notification is required to more than 1,000 residents.	Without unreasonable delay	
Minnesota	Minn. Stat. § 325E.61; Minn. Stat. § 13.055	For persons or businesses conducting business in Minnesota, notice is required following discovery or notification of a breach in the security of a system when the unencrypted personal information (defined in Minn. Stat. § 325E.61 subdivision 1(e)) was, or is reasonably believed to have been, acquired by an unauthorized person. A governmental entity that collects, creates, receives, maintains or disseminates private or confidential data on individuals must provide notice following discovery or notification of a breach, to any individual whose private or confidential data was, or is reasonably believed to have been, acquired by an unauthorized person.	Notice must be provided in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as outlined in Minn. Stat. § 325E.61(c) or Minn. Stat. § 13.055(3) as applicable, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system or, in the case of non-governmental systems, any measures necessary to identify the affected individuals.	Not required	Not applicable	Yes, for non-governmental entities, to consumer reporting agencies, if more than 500 persons must be notified at one time. For government entities, to consumer reporting agencies if notice is required to more than 1,000 people.	For non-governmental persons, within 48 hours. For government entities, without unreasonable delay.	

Private right of action

An individual or entity that maintains personal data that the individual or entity does not own or license (a vendor or other third party) that experiences a breach must notify the owner or licensor of the information.

Notice not required if data was encrypted and the decryption key was not compromised

Waiver of statutory provision void and unenforceable

State	Breach notification statute	Notification trigger	Notification time frame (individuals)	Notification to the state attorney general	Notification time frame (state attorney general)	Notification to other government agencies or consumer reporting agencies	Notification time frame (other government agencies or CRAs)	Additional features
Mississippi	Miss. Code § 75-24-29	A person who conducts business in Mississippi must disclose any breach of security, defined as the unauthorized acquisition of electronic files or computerized data containing unencrypted personal information (Miss. Code § 75-24-29), to all affected individuals. Disclosure 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.	Notice must be provided without unreasonable delay, subject to the completion of an investigation to determine the nature and scope of the incident, identify the affected individuals, or restore the reasonable integrity of the data system. Notification shall be delayed for a reasonable time upon law enforcement determination, as outlined in Miss. Code § 75-24-29(5).	Not required	Not applicable	Not required	Not applicable	* A data processor must notify an information owner or licensee of any breach if personal information was, or is reasonably believed to have been, acquired by an unauthorized person for fraudulent purposes.
Missouri	Mo. Rev. Stat. § 407.1500	Notice is required following the discovery or notification of a breach of security of personal information (defined in Mo. Rev. Stat. § 407.1500.1(9)) of a resident of Missouri maintained in computerized form. Notice is not required if, as outlined in Mo. Rev. Stat. § 407-1500.2(5), the person, after an appropriate investigation or consultation with law enforcement, determines that a risk of identity theft or other fraud to any consumer is not reasonably likely to occur.	Notice must be as expeditious as possible and without reasonable delay, consistent with the legitimate needs of law enforcement as provided in Mo. Rev. Stat. § 407.1500(2)(3), and consistent with any measures necessary to determine sufficient contact information and to determine the scope of the breach and restore the reasonable integrity, security and confidentiality of the data system.	Yes, notice to the state attorney general is required if notice is provided to more than 1,000 consumers at one time.	Without unreasonable delay	Yes, notification to consumer reporting agencies is required if notice is provided to more than 1,000 consumers at one time.	Without unreasonable delay	

Private right of action

An individual or entity that maintains personal data that the individual or entity does not own or license (a vendor or other third party) that experiences a breach must notify the owner or licensor of the information.

Notice not required if data was encrypted and the decryption key was not compromised

Waiver of statutory provision void and unenforceable

State	Breach notification statute	Notification trigger	Notification time frame (individuals)	Notification to the state attorney general	Notification time frame (state attorney general)	Notification to other government agencies or consumer reporting agencies	Notification time frame (other government agencies or CRAs)	Additional features
Montana	Mont. Code Ann. § 30-14-1701 et seq.	Notice is required following discovery or notification of a breach of security of computerized data, to any resident of Montana whose unencrypted personal information (defined in Mont. Code Ann. § 30-14-1704(4)(b)) was or is reasonably believed to have been acquired by an unauthorized person, where breach is defined as the unauthorized acquisition that causes or is reasonably believed to cause loss or injury to a Montana resident.	Notice must be provided without unreasonable delay, consistent with the legitimate needs of law enforcement as provided in Mont. Code Ann. § 30-14-1704(3) or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.	Yes	Simultaneous with notification to individual	Notification is not required but see Mont. Code Ann. § 30-14-1704(7) regarding coordination with consumer reporting agencies.	Not applicable	
Nebraska	Neb. Rev. Stat. §§ 87-801 et seq.	When an individual or commercial entity conducting business in Nebraska that owns or licenses computerized data that includes personal information (as defined in Neb. Rev. Stat. § 87-802(5)) about a resident of Nebraska becomes aware of a breach of the security of their system, they must conduct a reasonable and prompt investigation in good faith. Notice is required if that investigation determines that the use of personal information about a Nebraska resident for an unauthorized purpose has occurred or is likely to occur.	Notice must be provided as soon as possible and without unreasonable delay, consistent with the legitimate needs of law enforcement in accordance with Neb. Rev. Stat. § 87-803(4) and any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system.	Yes	Not later than the time when notice is provided to residents	Not required	Not applicable	
Nevada	Nev. Rev. Stat. §§ 603A.010 et seq.	Notice is required following the discovery or notification of a breach of security of a system of computerized data where unencrypted personal information (as defined in NRS 603A.040) of any resident of Nevada was, or is reasonably believed to have been, acquired by an unauthorized person.	Notice must be provided in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in NRS 603A.220(3) or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system data.	Not required	Not applicable	Yes, notification to consumer reporting agencies is mandatory if notice is required to more than 1,000 persons at any one time.	Without unreasonable delay	

Private right of action

An individual or entity that maintains personal data that the individual or entity does not own or license (a vendor or other third party) that experiences a breach must notify the owner or licensor of the information.

Notice not required if data was encrypted and the decryption key was not compromised

Waiver of statutory provision void and unenforceable

State	Breach notification statute	Notification trigger	Notification time frame (individuals)	Notification to the state attorney general	Notification time frame (state attorney general)	Notification to other government agencies or consumer reporting agencies	Notification time frame (other government agencies or CRAs)	Additional features
New Hampshire	N.H. Rev. Stat. Ann. § 359-C:20; see also N.H. Rev. Stat. Ann. § 332-I:5 for medical records	Notice is required upon determination that misuse of personal information (as defined in RSA § 359-C:19) has occurred or is reasonably likely to occur as a result of a security breach. This determination of the likelihood that the information has been or will be misused must be made promptly by a person doing business in the state when they become aware of a security breach. If no determination can be made, affected individuals should be notified. For health care providers and their business associates, notice is required if protected health information is disclosed in a manner prohibited under RSA § 332-I:4.	Notice must be provided as soon as possible/as quickly as possible after a determination of misuse, except that notice may be delayed based on the determination of a law enforcement, national security or homeland security agency as outlined in RSA § 359-C:20(II).	Yes, if the person is not engaged in trade or commerce that is subject to RSA § 358-A:3	Before notice is given to individuals	Yes, notification to the person's primary regulator is required if they are engaged in trade or commerce subject to RSA § 358-A:3. Notification to consumer reporting agencies is also mandatory if notice is required to more than 1,000 consumers.	For notice to the person's primary regulator, before notice to individuals. For notice to CRAs, without unreasonable delay.	
New Jersey	N.J. Stat. §§ 56:8-161 to -166	Notice is required following discovery or notification of any breach of security of computerized records where the personal information of any resident of New Jersey was or is reasonably believed to have been accessed by an unauthorized person, unless the business or public entity maintaining the records establishes that misuse of the information is not reasonably possible.	Notice must be provided in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement as provided in N.J. Stat. Ann. § 56:8-163(c)(2) or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.	Yes, to the Division of State Police in the Department of Law and Public Safety	In advance of disclosure to the customer	Yes, notification to consumer reporting agencies is mandatory if notice is required to more than 1,000 persons at one time.	Without unreasonable delay	
New Mexico	N.M. Stat. Ann. § 57-12C-6	Notice is required upon discovery or notification that personal identifying information (as defined in N.M. Stat. Ann. § 57-12C-2) of a New Mexico resident is reasonably believed to have been subject to a security breach, unless, after an appropriate investigation, the person determines that the security breach does not give rise to a significant risk of identity theft or fraud.	Notice must be provided in the most expedient time possible but no more than 45 days following discovery of the security breach, except as provided in N.M. Stat. Ann. § 57-12C-9 if a law enforcement agency determines that the notification will impede a criminal investigation or as necessary to determine the scope of the security breach and restore the integrity, security and confidentiality of the data system.	Yes, notice to the state attorney general is required if notification must be provided to more than 1,000 New Mexico residents as a result of a single security breach.	In the most expedient time possible, but no later than 45 days	Yes, notification to consumer reporting agencies is mandatory if notice is required to more than 1,000 New Mexico residents as a result of a single security breach.	In the most expedient time possible, but no later than 45 days	

 Private right of action

 An individual or entity that maintains personal data that the individual or entity does not own or license (a vendor or other third party) that experiences a breach must notify the owner or licensor of the information.

 Notice not required if data was encrypted and the decryption key was not compromised

 Waiver of statutory provision void and unenforceable

State	Breach notification statute	Notification trigger	Notification time frame (individuals)	Notification to the state attorney general	Notification time frame (state attorney general)	Notification to other government agencies or consumer reporting agencies	Notification time frame (other government agencies or CRAs)	Additional features
New York	N.Y. Gen. Bus. Law § 899-aa	Notice is required following discovery or notification of a breach of the security of the system, to any resident of New York state whose private information (defined in N.Y. Gen. Bus. Law § 899-aa) was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization. Disclosure is not necessary if the exposure of private information was inadvertent and the person or business reasonably determines it will not likely result in misuse of the information, or financial harm or emotional harm in the case of unknown disclosure of online credentials.	Notice must be provided in the most expedient time possible and without unreasonable delay, but within 30 days after the discovery. Notice may be delayed for the legitimate needs of law enforcement as outlined in N.Y. Gen. Bus. Law § 899-aa(4).	Yes, notice to the state attorney general is required if any New York residents are to be notified. Under N.Y. Gen. Bus. Law § 899-aa(2)(a), if an incident affecting over 500 residents is determined not likely to cause harm and notification to residents is not required, such determination must be provided to the state attorney general within 10 days after the determination.	Without delaying notice to residents	Yes, notification to the department of state and the division of state police is required. Also, if the person or business is a covered entity under 23 N.Y. Codes Rules & Regs. 500.1, notification is required to the department of financial services. If notification is required to the secretary of health and human services pursuant to HIPAA or the HITECH Act, notification is required to the state attorney general within five business days of notifying the secretary. To consumer reporting agencies if more than 5,000 New York residents are to be notified at one time.	Without delaying notice to residents	

Private right of action

An individual or entity that maintains personal data that the individual or entity does not own or license (a vendor or other third party) that experiences a breach must notify the owner or licensor of the information.

Notice not required if data was encrypted and the decryption key was not compromised

Waiver of statutory provision void and unenforceable

State	Breach notification statute	Notification trigger	Notification time frame (individuals)	Notification to the state attorney general	Notification time frame (state attorney general)	Notification to other government agencies or consumer reporting agencies	Notification time frame (other government agencies or CRAs)	Additional features
North Carolina	N.C. Gen. Stat. § 75-60 et seq.	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. Security breach is defined as an incident of unauthorized access to an acquisition of unencrypted and unredacted records or data 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. For purposes of this requirement, personal information shall not include electronic identification numbers, electronic mail names or addresses, Internet account numbers, Internet identification names, parent's legal surname prior to marriage, or a password unless this information would permit access to a person's financial account or resources.	Notice must be provided without unreasonable delay, consistent with the legitimate needs of law enforcement as outlined in N.C. Gen. Stat. § 75-65(c) and any measures necessary to determine sufficient contact information, determine the scope of the breach and restore the reasonable integrity, security and confidentiality of the data system.	Yes, notification to the Consumer Protection Division of the attorney general's office is required if a business provides notice to an affected person.	Without unreasonable delay	Yes, notification to consumer reporting agencies is required if a business provides notice to more than 1,000 persons at one time.	Without unreasonable delay	Under N.C Gen Stat. 75-1.1 and 75-16, by N.C. Gen. Stat. § 75-65(i), "if injured."
North Dakota	N.D. Cent. Code § 51-30-01 et seq.	Notice is required following the discovery or notification of a breach of the security system, defined as the unauthorized acquisition of unencrypted computerized data, to any resident of the state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.	Notice must be provided in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement as outlined in N.D. Cent. Code § 51-30-04 or any measures necessary to determine the scope of the breach and to restore the integrity of the data system.	Yes, notice to the state attorney general is required if the breach exceeds 250 individuals.	In the most expedient time possible without unreasonable delay	Not required	Not applicable	

Private right of action

An individual or entity that maintains personal data that the individual or entity does not own or license (a vendor or other third party) that experiences a breach must notify the owner or licensor of the information.

Notice not required if data was encrypted and the decryption key was not compromised

Waiver of statutory provision void and unenforceable

State	Breach notification statute	Notification trigger	Notification time frame (individuals)	Notification to the state attorney general	Notification time frame (state attorney general)	Notification to other government agencies or consumer reporting agencies	Notification time frame (other government agencies or CRAs)	Additional features
Ohio	Ohio Rev. Code Ann. § 1349.19	Notice is required following discovery or notification of a breach of the security of a system to any resident of Ohio 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 is reasonably believed will cause a material risk of identity theft or other fraud to the resident.	Notice must be provided in the most expedient time possible but no more than 45 days following the discovery or notification of the breach, subject to the legitimate needs of law enforcement as outlined in Ohio Rev. Code Ann. § 1349.19(D) and consistent with measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.	Not required	Not applicable	Yes, notification to consumer reporting agencies is required if circumstances require notice to more than 1,000 residents involved in a single occurrence of a breach.	Without unreasonable delay	
Oklahoma	Okla. Stat. tit. 24, § 161 et seq.	Notice is required following the determination or notification of a breach of the security of a system of computerized data to a resident of Oklahoma 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 the state.	Notice must be provided without reasonable delay except for the legitimate needs of law enforcement as outlined in Okla. Stat. tit. 24, § 163(D) or in order to take any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system.	Yes, notice to the state attorney general is required when a single breach affects 500 or more residents of the state, except for credit bureaus where the threshold is 1,000 residents or more.	Without unreasonable delay but in no event more than 60 days after providing notice to state residents	Not required	Not applicable	

Private right of action

An individual or entity that maintains personal data that the individual or entity does not own or license (a vendor or other third party) that experiences a breach must notify the owner or licensor of the information.

Notice not required if data was encrypted and the decryption key was not compromised

Waiver of statutory provision void and unenforceable

State	Breach notification statute	Notification trigger	Notification time frame (individuals)	Notification to the state attorney general	Notification time frame (state attorney general)	Notification to other government agencies or consumer reporting agencies	Notification time frame (other government agencies or CRAs)	Additional features
Oregon	Or. Rev. Stat. §§ 646A.600 - 646A.604	Notice is required upon notice or discovery of a breach of security, defined as "an unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information that a person maintains or possesses." Disclosure is not necessary if, after an appropriate investigation or consultation with relevant federal, state or local law enforcement agencies, the covered entity reasonably determines that the consumers whose personal information was subject to the breach of security are unlikely to suffer harm.	Notice must be provided in the most expeditious manner possible, without unreasonable delay, but no later than 45 days after discovering or receiving notification of the breach. Notice may be delayed if law enforcement requests in writing that the covered entity delay the notification as outlined in Or. Rev. Stat. § 646A.604(3)(c). Before providing notice, a covered entity shall undertake reasonable measures that are necessary to determine sufficient contact information for the intended recipient of the notice; determine the scope of the breach of security; and restore the reasonable integrity, security and confidentiality of the personal information.	Yes, notice to the state attorney general is required if notice must be sent to more than 250 consumers. Vendors discovering a breach must notify the attorney general if the breach involved the personal information of more than 250 consumers or a number of consumers that the vendor could not determine unless the covered entity has notified the attorney general.	Without unreasonable delay, no later than 45 days after the discovery or notification of the breach.	Yes, notification to consumer reporting agencies is required if the breach affects 1,000 or more consumers.	Without unreasonable delay	
Pennsylvania	73 Pa. Stat. §§ 2301 et seq.	Notice is required when it is determined that a breach of system security has occurred involving any resident of Pennsylvania whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person. For the purposes of this requirement, breach is defined as the "unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of personal information … and that causes or the entity reasonably believes has caused or will cause loss or injury to any resident" of the state (73 Pa. Stat. § 2302).	Notice must be provided without unreasonable delay, except upon the determination and advice of law enforcement, as outlined in 73 Pa. Stat. § 2304. Notice may also be delayed in order to take any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. If a state agency determines that it is the subject of a breach, it shall provide notice within seven business days following determination of the breach.	Yes, notice to the state attorney general is required if notice must be given to more than 500 individuals in Pennsylvania or if a state agency determines that it is the subject of a breach of the security of the system affecting personal information maintained by the state agency or state agency contractor.	Concurrently with notice to individuals	Yes, notification to consumer reporting agencies is required if notice must be provided to more than 500 individuals.	Without unreasonable delay	

Private right of action

An individual or entity that maintains personal data that the individual or entity does not own or license (a vendor or other third party) that experiences a breach must notify the owner or licensor of the information.

Notice not required if data was encrypted and the decryption key was not compromised

Waiver of statutory provision void and unenforceable

State	Breach notification statute	Notification trigger	Notification time frame (individuals)	Notification to the state attorney general	Notification time frame (state attorney general)	Notification to other government agencies or consumer reporting agencies	Notification time frame (other government agencies or CRAs)	Additional features
Rhode Island	R.I. Gen. Laws §§ 11-49.3-1 to -7	Notice is required following any disclosure of personal information or any breach of the security of a system that poses a significant risk of identity theft to any resident of Rhode Island whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person or entity.	For persons that are not a state or municipal agency, notice must be provided in the most expedient time possible but no more than 45 days after confirmation of the breach and the ability to ascertain the information required to fulfill the notice requirements, unless law enforcement determines that the notification will impede a criminal investigation. See R.I. Gen. Laws § 11-49.3-4(b). For state and municipal agencies, notice must be provided no more than 30 days after confirmation of the breach.	Yes, notice to the state attorney general is required if more than 500 Rhode Island residents are to be notified.	Without delaying notice to residents	Yes, notification to the major credit reporting agencies is required if more than 500 Rhode Island residents are to be notified. Any municipal agency or state agency that detects a cybersecurity incident shall provide notification to the Rhode Island state police upon detection of the incident within 24 hours.	Without delaying notice to residents	
South Carolina	S.C. Code § 39-1-90	Notification is required following discovery or notification of a breach of the security of a system in which a South Carolina resident's unencrypted personal identifying information, as defined in S.C. Code § 39-1-90(D)(3), 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.	Notice must be provided in the most expedient time possible and without unreasonable delay. However, notice may be delayed if law enforcement determines that the notification impedes a criminal investigation, as provided in S.C. Code § 39-1-90(C) or consistent with measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.	Not required	Not applicable	Yes, notification to the Consumer Protection Division of the Department of Consumer Affairs and to consumer reporting agencies is required if a business provides notice to more than 1,000 persons.	Without unreasonable delay	
South Dakota	S.D. Codified Laws §§ 22-40-19 to -26	Following the discovery or notification of a breach of system security, notice is required to any resident of South Dakota whose personal or protected information was, or is reasonably believed to have been, acquired by an unauthorized person unless, following an appropriate investigation and notice to the attorney general, the information holder reasonably determines that the breach will not likely result in harm to the affected person.	Notice must be provided no later than 60 days from discovery or notification, unless a law enforcement agency determines that the notification will impede a criminal investigation, as provided under S.D. Codified Laws § 22-40-21.	Yes, notice to the state attorney general is required if the breach exceeds 250 residents of the state.	Not specified	Yes, notification to consumer reporting agencies is mandatory if notice is required under S.D. Codified Laws § 22-40-20.	Without unreasonable delay	

Private right of action

An individual or entity that maintains personal data that the individual or entity does not own or license (a vendor or other third party) that experiences a breach must notify the owner or licensor of the information.

Notice not required if data was encrypted and the decryption key was not compromised

Waiver of statutory provision void and unenforceable

State	Breach notification statute	Notification trigger	Notification time frame (individuals)	Notification to the state attorney general	Notification time frame (state attorney general)	Notification to other government agencies or consumer reporting agencies	Notification time frame (other government agencies or CRAs)	Additional features
Tennessee	Tenn. Code Ann. §§ 47-18-2105 to -2107	Following discovery or notification of a breach of system security, an information holder must disclose the breach to any resident of Tennessee whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person.	Notice must be provided no later than 45 days from the discovery or notification of the breach, unless law enforcement determines that the notification will impede a criminal investigation. See Tenn. Code Ann. § 47-18-2107(d).	Not required	Not applicable	Yes, notification to consumer reporting agencies is required if notification is required to more than 1,000 persons.	Without unreasonable delay	
Texas	Tex. Bus. & Com. Code Ann. § 521.053	After discovering or receiving notification of any breach of system security, notice is required to any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person.	Notice must be provided without unreasonable delay and not later than the 60th day after the date on which the person determines that the breach occurred, unless law enforcement determines that the notification will impede a criminal investigation, as provided in Tex. Bus. & Com. Code Ann. § 521.053(d) or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system.	Yes, notice to the state attorney general is required if the breach involves at least 250 Texas residents.	As soon as practicable and not later than the 30th day after the date on which the person determines that the breach occurred	Yes, notification to consumer reporting agencies is mandatory if notice is required to more than 10,000 persons.	Without unreasonable delay	
Utah	Utah Code § 13-44-202	Notice is required if a reasonable and prompt investigation, which a person who owns or licenses computerized data that includes personal information concerning a Utah resident must conduct in good faith when the person becomes aware of a breach of system security, reveals that the misuse of personal information for identity theft or fraud purposes has occurred, or is reasonably likely to occur.	Notice must be provided in the most expedient time possible without unreasonable delay, considering the legitimate needs of law enforcement, as provided under Utah Code § 13-44-202(4)(a) and after determining the scope of the breach of the system security and restoring the reasonable integrity of the system. See Utah Code § 13-44-202(2)(a)-(c).	Yes, notice to the office of the attorney general and the Utah Cyber Center is required if investigation reveals the misuse of personal information relating to 500 or more Utah residents for identity theft or fraud purposes has occurred or is reasonably likely to occur.	In the most expedient time possible without unreasonable delay, considering legitimate investigative needs of law enforcement and after determining the scope of the breach and after restoring the reasonable integrity of the system	Yes, notification to consumer reporting agencies is required if investigation reveals that the misuse of personal information relating to 1,000 or more Utah residents for identity theft or fraud purposes has occurred or is reasonably likely to occur.	In the most expedient time possible without unreasonable delay, considering legitimate investigative needs of law enforcement and after determining the scope of the breach and after restoring the reasonable integrity of the system	

Private right of action

An individual or entity that maintains personal data that the individual or entity does not own or license (a vendor or other third party) that experiences a breach must notify the owner or licensor of the information.

Notice not required if data was encrypted and the decryption key was not compromised

Waiver of statutory provision void and unenforceable

State	Breach notification statute	Notification trigger	Notification time frame (individuals)	Notification to the state attorney general	Notification time frame (state attorney general)	Notification to other government agencies or consumer reporting agencies	Notification time frame (other government agencies or CRAs)	Additional features
Vermont	9 V.S.A.§ 2435	Notice is required following discovery or notification of a security breach of computerized personally identifiable information or login credentials of a customer unless, as outlined in 9 V.S.A § 2435(d), the data collector establishes that misuse of personally identifiable information or login credentials is not reasonably possible. If the data collector subsequently obtains facts indicating that misuse of the personally identifiable information or login credentials has occurred or is occurring, the data collector shall provide notice.	Notice must be provided in the most expedient time possible and without unreasonable delay but not later than 45 days after the discovery or notification of the breach, consistent with the legitimate needs of law enforcement, as provided in 9 V.S. A. § 2435(b)(3) and (4), or with any measures necessary to determine the scope of the security breach and restore the reasonable integrity, security and confidentiality of the data system.	Yes, notification is required to the attorney general or, in the case of an entity regulated by the Department of Financial Regulation, to such department, as provided in 9 V.S.A. § 2435(b)(3)(A). If the data collector establishes that misuse of the personally identifiable information or login credentials is not reasonably possible, the data collector shall provide notice of its determination and a detailed explanation for said determination to the attorney general or to the Department of Financial Regulation.	Within 14 business days of the data collector's discovery of the security breach, consistent with the legitimate needs of law enforcement, or when the data collector provides notice to consumers, whichever is sooner	Yes, notification to consumer reporting agencies is required if a data collector provides notice to more than 1,000 consumers at one time.	Without unreasonable delay	

Private right of action

An individual or entity that maintains personal data that the individual or entity does not own or license (a vendor or other third party) that experiences a breach must notify the owner or licensor of the information.

Notice not required if data was encrypted and the decryption key was not compromised

Waiver of statutory provision void and unenforceable

State	Breach notification statute	Notification trigger	Notification time frame (individuals)	Notification to the state attorney general	Notification time frame (state attorney general)	Notification to other government agencies or consumer reporting agencies	Notification time frame (other government agencies or CRAs)	Additional features
Virginia	Va. Code § 18.2-186.6	Following the discovery or notification of a breach of the security of a system, notice is required 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 fraud to any resident of Virginia.	Notice must be provided without unreasonable delay. Notice may be reasonably delayed to allow the individual or entity to determine the scope of the breach of the security of the system and restore the reasonable integrity of the system and if a law enforcement agency determines and advises the individual or entity that the notice will impede a criminal or civil investigation, or homeland or national security, as outlined in Va. Code § 18.2-186.6(B).	Yes	Notice is required without unreasonable delay. Notice may be reasonably delayed to allow the individual or entity to determine the scope of the breach of the security of the system and restore the reasonable integrity of the system and if a law-enforcement agency determines and advises the individual or entity that the notice will impede a criminal or civil investigation, or homeland or national security. subject to the needs of law enforcement as outlined in Va. Code § 18.2-186.6(B).	Yes, notification to consumer reporting agencies is required if notice is provided to more than 1,000 persons at one time.	Without unreasonable delay	
Washington	Wash. Rev. Code §§ 19.255.010 et seq.	Following any breach of the security of a system (defined in RCW 19.255.005), notice is required to any resident of Washington whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person, where the information was not secured, unless the breach is not reasonably likely to subject consumers to a risk of harm.	Notice must be provided in the most expedient time possible, without unreasonable delay, and no more than 30 days after the breach was discovered, unless a law enforcement agency determines that the notification will impede a criminal investigation, as provided in RCW 19.255.010(3), or the delay is due to any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.	Yes, notification is mandatory if notice is required to more than 500 Washington residents as a result of a single breach.	No more than 30 days after the breach was discovered	Not required	Not applicable	

 Private right of action

 An individual or entity that maintains personal data that the individual or entity does not own or license (a vendor or other third party) that experiences a breach must notify the owner or licensor of the information.

 Notice not required if data was encrypted and the decryption key was not compromised

 Waiver of statutory provision void and unenforceable

State	Breach notification statute	Notification trigger	Notification time frame (individuals)	Notification to the state attorney general	Notification time frame (state attorney general)	Notification to other government agencies or consumer reporting agencies	Notification time frame (other government agencies or CRAs)	Additional features
West Virginia	W. Va. Code §§ 46A-2A-101 et seq.	Notice is required following discovery or notification of a breach of the security of a system, defined as 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 the individual or entity reasonably believes has caused or will cause identity theft or other fraud to any resident of West Virgina.	Notice must be provided without unreasonable delay, except in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the system, or, as provided in W. Va. Code § 46A-2A-102(e), if a law enforcement determines and advises the individual or entity that the notice will impede a criminal or civil investigation or homeland or national security.	Not required	Not applicable	Yes, notification to consumer reporting agencies is mandatory if an entity is required to notify more than 1,000 persons.	Without unreasonable delay	
Wisconsin	Wis. Stat. § 134.98	Notice is required if an entity knows that personal information in its possession has been acquired by a person whom the entity has not authorized to acquire the personal information, unless the acquisition does not create a material risk of identity theft or fraud to the data subject.	Notice must be provided within a reasonable time, not to exceed 45 days after learning of the acquisition of personal information, subject to the request of law enforcement as provided in Wis. Stat. § 134.98(5).	Not required	Not applicable	Yes, notification to consumer reporting agencies is mandatory if an entity is required to notify 1,000 or more individuals.	Without unreasonable delay	* *Failure to comply with this section is not negligence or a breach of any duty, but may be evidence of negligence or a breach of a legal duty (Wis. Stat. § 134.98(4)).

Private right of action

An individual or entity that maintains personal data that the individual or entity does not own or license (a vendor or other third party) that experiences a breach must notify the owner or licensor of the information.

Notice not required if data was encrypted and the decryption key was not compromised

Waiver of statutory provision void and unenforceable

State	Breach notification statute	Notification trigger	Notification time frame (individuals)	Notification to the state attorney general	Notification time frame (state attorney general)	Notification to other government agencies or consumer reporting agencies	Notification time frame (other government agencies or CRAs)	Additional features
Wyoming	Wyo. Stat. §§ 40-12-501 to -502	An individual or commercial entity that conducts business in Wyoming and owns or licenses computerized data that includes personal identifying information about a resident of the state must conduct a reasonable and prompt investigation in good faith when it becomes aware of a breach of the security of the system. Notice is required if that investigation determines that the misuse of personal identifying information about a Wyoming resident has occurred or is reasonably likely to occur.	Notice must be provided as soon as possible, in the most expedient time possible, and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in Wyo. Stat. § 40-12-502(b), and any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.	Not required	Not applicable	Not required	Not applicable	
District of Columbia	D.C. Code § 28-3851 et seq.	Notice is required upon discovery of a breach of the security of a system, as defined in D.C. Code § 28-3851, where the personal information of a District of Columbia resident was included in the breach.	Notice must be provided in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in D.C. Code § 28-3852(d), and with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.	Yes, notice to the attorney general is required if the breach affects 50 or more D.C. residents.	Promptly, in the most expedient manner possible, without unreasonable delay, and not later than when notice is provided to residents	Yes, notification to all consumer reporting agencies is required if more than 1,000 individuals are notified.	Without unreasonable delay	
Guam	9 Guam Code §§ 48.10 to 48.80	Following discovery or notification of a breach of the security of a system, notice is required to any resident of Guam whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person and that causes or that the data owner or licensee reasonably believes has caused or will cause identity theft or other fraud to any resident of Guam.	Notice must be provided as expeditiously as possible and without unreasonable delay, except as determined by law enforcement, as provided in 9 Guam Code § 48.30(d), or in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the system.	Not required	Not applicable	Not required	Not applicable	

Private right of action

An individual or entity that maintains personal data that the individual or entity does not own or license (a vendor or other third party) that experiences a breach must notify the owner or licensor of the information.

Notice not required if data was encrypted and the decryption key was not compromised

Waiver of statutory provision void and unenforceable

State	Breach notification statute	Notification trigger	Notification time frame (individuals)	Notification to the state attorney general	Notification time frame (state attorney general)	Notification to other government agencies or consumer reporting agencies	Notification time frame (other government agencies or CRAs)	Additional features
Puerto Rico	P.R. Laws Ann. tit. 10, §§ 4051 et seq.	Notice is required when a database whose security has been breached contains, in whole or in part, personal information files of citizens residents of Puerto Rico and that information is not protected by an encrypted code but only by a password.	Notice must be provided as expeditiously as possible, taking into consideration the needs 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.	Not required	Not applicable	Yes, notification to the Department of Consumer Affairs is required.	Within 10 days after the violation of the system's security has been detected	
U.S. Virgin Islands	V.I. Code Ann. tit. 14, §§ 2208 et seq.	Following discovery or notification of a breach in the security of computerized data that includes personal information, notice must be provided to any resident of the Virgin Islands whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.	Notice must be provided in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in V.I. Code Ann. tit. 14, § 2208(c) and § 2209(c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.	Not required	Not applicable	Not required	Not applicable	

Private right of action

An individual or entity that maintains personal data that the individual or entity does not own or license (a vendor or other third party) that experiences a breach must notify the owner or licensor of the information.

Notice not required if data was encrypted and the decryption key was not compromised

Waiver of statutory provision void and unenforceable

Contact

Jim Dempsey
Managing Director, IAPP Cybersecurity Law Center
jdempsey@iapp.org

For further inquiries, please reach out to research@iapp.org.

Follow the IAPP on social media

Updated February 2026.