State	Vendor Cooperation or Notice Requirement
Alabama	Under Ala. Code § 8-38-8, in the event a third-party agent has experienced a breach of security in the system maintained by the agent, the agent shall notify the covered entity of the breach of security as expeditiously as possible and without unreasonable delay, but no later than 10 days following the determination of the breach of security or reason to believe the breach occurred. After receiving notice from a third-party agent, a covered entity shall provide notices required under Sections 8-38-5 and 8-38-6. A third-party agent, in cooperation with a covered entity, shall provide information in the possession of the third-party agent so that the covered entity can comply with its notice requirements. A covered entity may enter into a contractual agreement with a third-party agent whereby the third-party agent agrees to handle notifications required under this chapter.
Alaska	Under Alaska Stat. § 45.48.070, if an entity experiences a breach of security of personal information that it does not own or license, it shall notify the entity that owns or licensed the use of the personal information about the breach and cooperate as necessary to allow that entity to comply with its statutory obligations. Notifications must be made in the most expeditious time possible and without unreasonable delay.
Arizona	Under Ariz. Rev. Stat. § 18-552(C), a person that maintains unencrypted and unredacted computerized personal information that the person does not own or license shall notify, as soon as practicable, the owner or licensee of the information on discovering any security system breach and cooperate with the owner or the licensee of the personal information, including sharing information relevant to the breach with the owner or licensee.
Arkansas	Under Ark. Code § 4-110-105(b), if an entity maintains computerized data that includes personal information that the entity does not own, the entity shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Notifications must be made in the most expedient time and manner possible and without unreasonable delay.
California	Under Cal. Civ. Code § 1798.82(b), if an entity maintains computerized data that includes personal information that the entity does not own, the entity must notify the owner or licensee of the information of any breach of the security of the data immediately following discovery if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Notifications must be made in the most expedient time possible and without unreasonable delay.
Colorado	Under Colo. Rev. Stat. § 6-1-716(2)(b), if a covered entity uses a third-party service provider to maintain computerized data that includes personal information, then the third-party service provider shall give notice to and cooperate with the covered entity in the event of a security breach that compromises such computerized data, including notifying the covered entity of any security breach in the most expedient time possible, and without unreasonable delay following discovery of a security breach, if misuse of personal information about a Colorado resident occurred or is likely to occur. Cooperation includes sharing with the covered entity information relevant to the security breach; except that such cooperation does not require the disclosure of confidential business information or trade secrets.
Connecticut	Under Conn. Gen. Stat. § 36a-701b(b)(3), if an entity maintains personal information that the entity does not own, it must notify the owner or licensee of the information of any breach of the security of the data immediately following discovery if the personal information was, or is reasonably believed to have been, breached.
Delaware	Under Del. Code tit. 6 § 12B-102(b), a person that maintains computerized data that includes personal information that the person does not own or license shall give notice to and cooperate with the owner or licensee of the information of any breach of security immediately following determination of the breach of security. For purposes of this subsection, "cooperation" includes sharing with the owner or licensee information relevant to the breach.
Florida	Under Fla. Stat. § 501.171(6), any third-party agent shall disclose to the covered entity for which the information is maintained any breach of the security of the system as expeditiously as practicable, but no later than 10 days following the determination of the breach or reason to believe the breach occurred. The third-party agent must provide the covered entity with all information necessary to comply with the notice requirements.
Georgia	Under Ga. Code Ann. § 10-1-912(b), any person or business that maintains computerized data on behalf of an information broker or data collector that includes personal information of individuals that the person or business does not own shall notify the information broker or data collector of any breach of the security of the system within 24 hours following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
Hawaii	Under Haw. Rev. Stat. § 487N-2(b), any business located in Hawaii or any business that conducts business in Hawaii that maintains or possesses records or data containing personal information of residents of Hawaii that the business does not own or license, or any government agency that maintains or possesses records or data containing personal information of residents of Hawaii shall notify the owner or licensee of the information of any security breach immediately following discovery of the breach.

Idaho	Under Idaho Code § 28-51-105(2), if an entity maintains computerized data that includes personal information that the entity does not own or license, it must notify the owner or licensee of the information of any breach of the security of the system immediately following discovery if misuse of personal information about an Idaho resident occurred or is reasonably likely to occur. Cooperation includes sharing relevant information about the breach.
Illinois	Under 815 ILCS 530/10(b), any data collector that maintains or stores, but does not own or license, computerized data that includes personal information that the data collector does not own or license shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. In addition to providing such notification to the owner or licensee, the data collector shall cooperate with the owner or licensee in matters relating to the breach. That cooperation shall include, but need not be limited to, (i) informing the owner or licensee of the breach, including giving notice of the date or approximate date of the breach and the nature of the breach, and (ii) informing the owner or licensee of any steps the data collector has taken or plans to take relating to the breach. The data collector's cooperation shall not, however, be deemed to require either the disclosure of confidential business information or trade secrets or the notification of an Illinois resident who may have been affected by the breach.
Indiana	Under Ind. Code § 24-4.9-3-2, a person that maintains computerized data but that is not a data base owner shall notify the data base owner if the person discovers that personal information was or may have been acquired by an unauthorized person.
Iowa	Under Iowa Code § 715C.2(2), any person who maintains or otherwise possesses personal information on behalf of another person shall notify the owner or licensor of the information of any breach of security immediately following discovery of such breach of security if a consumer’s personal information was included in the information that was breached.
Kansas	Under Kan. Stat. § 50-7a02(b), an individual or a commercial entity that maintains computerized data that includes personal information that the individual or the commercial entity does not own or license shall give notice to the owner or licensee of the information of any breach of the security of the data following discovery of a breach, if the personal information was, or is reasonably believed to have been, accessed and acquired by an unauthorized person.
Kentucky	Under Ky. Rev. Stat. § 365.732(3), any information holder that maintains computerized data that includes personally identifiable information that the information holder does not own shall notify the owner or licensee of the information of any breach of the security of the data as soon as reasonably practicable following discovery, if the personally identifiable information was, or is reasonably believed to have been, acquired by an unauthorized person.
Louisiana	Under La. Rev. Stat. § 51:3074(D), any agency or person that maintains computerized data that includes personal information that the agency or person does not own shall notify the owner or licensee of the information if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person through a breach of security of the system containing such data, following discovery by the agency or person of a breach of security of the system.
Maine	Under 10 Me. Rev. Stat. § 1348(2), a third party that maintains computerized data that includes personal information on behalf of another entity must notify the owner or licensee of the information immediately following discovery of a breach if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
Maryland	Under Md. Code Com. Law § 14-3504(c)(1), a business that maintains computerized data that includes personal information of an individual residing in the State that the business does not own or license, when it discovers or is notified of a breach of the security of a system, shall notify, as soon as practicable, the owner or licensee of the personal information of the breach of the security of a system. Notification must be given as soon as reasonably practicable, but not later than 10 days after the business discovers or is notified of the breach. The business shall share information relative to the breach with the owner or licensee.
Massachusetts	Under Mass. Gen. Laws ch. 93H, § 3(a), a person or agency that maintains or stores, but does not own or license data that includes personal information about a resident of the commonwealth, shall provide notice, as soon as practicable and without unreasonable delay, when such person or agency (1) knows or has reason to know of a breach of security or (2) when the person or agency knows or has reason to know that the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose, to the owner or licensor in accordance with this chapter. In addition to providing notice as provided herein, such person or agency shall cooperate with the owner or licensor of such information. Such cooperation shall include, but not be limited to, informing the owner or licensor of the breach of security or unauthorized acquisition or use, the date or approximate date of such incident and the nature thereof, and any steps the person or agency has taken or plans to take relating to the incident, except that such cooperation shall not be deemed to require the disclosure of confidential business information or trade secrets, or to provide notice to a resident that may have been affected by the breach of security or unauthorized acquisition or use.
Michigan	Under Mich. Comp. Laws § 445.72(2), unless the person or agency determines that the security breach has not or is not likely to cause substantial loss or injury to, or result in identity theft with respect to, 1 or more residents of this state, a person or agency that maintains a database that includes data that the person or agency does not own or license that discovers a breach of the security of the database shall provide a notice to the owner or licensor of the information of the security breach.

Minnesota	Under Minn. Stat. § 325E.61(b), any person or business that maintains data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
Mississippi	Under Miss. Code § 75-24-29(4), any person who conducts business in this state that maintains computerized data which includes personal information that the person does not own or license shall notify the owner or licensee of the information of any breach of the security of the data as soon as practicable following its discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person for fraudulent purposes.
Missouri	Under Mo. Rev. Stat. § 407.1500.2.(2), any person that maintains or possesses records or data containing personal information of residents of Missouri that the person does not own or license, or any person that conducts business in Missouri that maintains or possesses records or data containing personal information of a resident of Missouri that the person does not own or license, shall notify the owner or licensee of the information of any breach of security immediately following discovery of the breach, consistent with the legitimate needs of law enforcement as provided in this section.
Montana	Under Mont. Code Ann. § 30-14-1704(2), any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data system immediately following discovery if the personal information was or is reasonably believed to have been acquired by an unauthorized person.
Nebraska	Under Neb. Rev. Stat. § 87-803(3), an individual or a commercial entity that maintains computerized data that includes personal information that the individual or commercial entity does not own or license shall give notice to and cooperate with the owner or licensee of the information of any breach of the security of the system when it becomes aware of a breach if use of personal information about a Nebraska resident for an unauthorized purpose occurred or is reasonably likely to occur. Cooperation includes, but is not limited to, sharing with the owner or licensee information relevant to the breach, not including information proprietary to the individual or commercial entity.
Nevada	Under Nev. Rev. Stat. § 603A.220(2), any data collector that maintains computerized data which includes personal information that the data collector does not own shall notify the owner or licensee of the information of any breach of the security of the system data immediately following discovery if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
New Hampshire	Under N.H. Rev. Stat. § 359-C:20(c), any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify and cooperate with the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was acquired by an unauthorized person.
New Jersey	Under N.J. Stat. Ann. § 56:8-163, any business or public entity that compiles or maintains computerized records that include personal information on behalf of another business or public entity shall notify that business or public entity, who shall notify its New Jersey customers, as provided in subsection a. of this section, of any breach of security of the computerized records immediately following discovery, if the personal information was, or is reasonably believed to have been, accessed by an unauthorized person.
New Mexico	Under N.M. Stat. Ann. § 57-12C-6(C), any person that is licensed to maintain or possess computerized data containing personal identifying information of a New Mexico resident that the person does not own or license shall notify the owner or licensee of the information of any security breach in the most expedient time possible, but not later than forty-five calendar days following discovery of the breach, except as provided in Section 9 of the Data Breach Notification Act; provided that notification to the owner or licensee of the information is not required if, after an appropriate investigation, the person determines that the security breach does not give rise to a significant risk of identity theft or fraud.
New York	Under N.Y. Gen. Bus. Law § 899-aa(2), any person or business which conducts business in New York state, and which owns or licenses computerized data which includes private information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of New York state whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision four of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system.
North Carolina	Under N.C. Gen. Stat. § 75-65(b), any business that maintains or possesses records or data containing personal information of residents of North Carolina that the business does not own or license, or any business that conducts business in North Carolina that maintains or possesses records or data containing personal information that the business does not own or license shall notify the owner or licensee of the information of any security breach immediately following discovery of the breach, consistent with the legitimate needs of law enforcement as provided in subsection (c) of this section.
North Dakota	Under N.D. Cent. Code § 51-30-03, any person that maintains computerized data that includes personal information that the person does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following the discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Ohio	Under Ohio Rev. Code § 1349.19(C), any person that, on behalf of or at the direction of another person or on behalf of or at the direction of any governmental entity, is the custodian of or stores computerized data that includes personal information shall notify that other person or governmental entity of any breach of the security of the system in an expeditious manner, if the personal information was, or reasonably is believed to have been, accessed and acquired by an unauthorized person and if the access and acquisition by the unauthorized person causes or reasonably is believed will cause a material risk of identity theft or other fraud to a resident of this state.
Oklahoma	Under Okla. Stat. § 24-163(C), an individual or entity that maintains computerized data that includes personal information that the individual or entity does not own or license shall notify the owner or licensee of the information of any breach of the security of the system as soon as practicable following discovery, if the personal information was or if the entity reasonably believes was accessed and acquired by an unauthorized person.
Oregon	Under Or. Rev. Stat. § 646A.604(2), a vendor that discovers a breach of security or has reason to believe that a breach of security has occurred shall notify a covered entity with which the vendor has a contract as soon as is practicable but not later than 10 days after discovering the breach of security or having a reason to believe that the breach of security occurred. If the breach involved the personal information of more than 250 consumers or a number of consumers that the vendor could not determine, the vendor must also notify the Attorney General. This requirement ensures timely compliance with notification responsibilities, allowing data owners to take necessary actions to protect affected individuals and secure the data.
Pennsylvania	Under 73 Pa. Stat. § 2303(c), a vendor that maintains, stores or manages computerized data on behalf of another entity shall provide notice of any breach of the security of the system following discovery by the vendor to the entity on whose behalf the vendor maintains, stores or manages the data. The entity shall be responsible for making the determinations and discharging any remaining duties under this act.
Rhode Island	N/A. While there is no explicit requirement for vendors to notify the data owner in the event of a breach, other responsibilities may still be applicable.
South Carolina	Under S.C. Code § 39-1-90(B), a person conducting business in this State and maintaining computerized data or other data that includes personal identifying information that the person does not own shall notify the owner or licensee of the information of a breach of the security of the data immediately following discovery, if the personal identifying information was, or is reasonably believed to have been, acquired by an unauthorized person.
South Dakota	N/A. No explicit requirement for vendors to notify the data owner in the event of a breach.
Tennessee	Under Tenn. Code § 47-18-2107(c), any information holder that maintains computerized data that includes personal information that the information holder does not own shall notify the owner or licensee of the information of any breach of system security if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made no later than forty-five (45) days from the discovery or notification of the breach of system security, unless a longer period of time is required due to the legitimate needs of law enforcement.
Texas	Under Tex. Bus. & Com. Code § 521.053(c), any person who maintains computerized data that includes sensitive personal information not owned by the person shall notify the owner or license holder of the information of any breach of system security immediately after discovering the breach, if the sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
Utah	Under Under Utah Code § 13-44-202(3), a person who maintains computerized data that includes personal information that the person does not own or license shall notify and cooperate with the owner or licensee of the information of any breach of system security immediately following the person's discovery of the breach if misuse of the personal information occurs or is reasonably likely to occur. Cooperation includes sharing information relevant to the breach with the owner or licensee of the information.
Vermont	Under 9 V.S.A. § 2435(b)(2), any data collector that maintains or possesses computerized data containing personally identifiable information or login credentials that the data collector does not own or license or any data collector that acts or conducts business in Vermont that maintains or possesses records or data containing personally identifiable information or login credentials that the data collector does not own or license shall notify the owner or licensee of the information of any security breach immediately following discovery of the breach, consistent with the legitimate needs of law enforcement.
Virginia	Under Va. Code § 18.2-186.6.(D), an individual or entity that maintains computerized data that includes personal information that the individual or entity does not own or license shall notify the owner or licensee of the information of any breach of the security of the system without unreasonable delay following discovery of the breach of the security of the system, if the personal information was accessed and acquired by an unauthorized person or the individual or entity reasonably believes the personal information was accessed and acquired by an unauthorized person.

Washington	Under Wash. Rev. Code § 19.255.010(2), any person or business that maintains data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
West Virginia	Under W. Va. Code § 46A-2A-102(b), an individual or entity that maintains computerized data that includes personal information that the individual or entity does not own or license shall give notice to the owner or licensee of the information of any breach of the security of the system as soon as practicable following discovery, if the personal information was or the entity reasonably believes was accessed and acquired by an unauthorized person.
Wisconsin	Under Wis. Stat. § 134.98(2)(bm), if a person, other than an individual, that stores personal information pertaining to a resident of this state, but does not own or license the personal information, knows that the personal information has been acquired by a person whom the person storing the personal information has not authorized to acquire the personal information, and the person storing the personal information has not entered into a contract with the person that owns or licenses the personal information, the person storing the personal information shall notify the person that owns or licenses the personal information of the acquisition as soon as practicable.
Wyoming	Under Wyo. Stat. Ann. § 40-12-502(g), any person who maintains computerized data that includes personal identifying information on behalf of another business entity shall disclose to the business entity for which the information is maintained any breach of the security of the system as soon as practicable following the determination that personal identifying information was, or is reasonably believed to have been, acquired by an unauthorized person. The person who maintains the data on behalf of another business entity and the business entity on whose behalf the data is maintained may agree which person or entity will provide any required notice as provided in subsection (a) of this section, provided only a single notice for each breach of the security of the system shall be required. If agreement regarding notification cannot be reached, the person who has the direct business relationship with the resident of this state shall provide notice.