Data Security Breaches:
Legislative/Regulatory Tracking Chart

(as of September 13, 2018)

All 50 states and DC have implemented data security breach laws. Specific provisions on existing laws can be found here.

This year South Dakota became the last state to adopt a data security breach law. Despite all states having laws, many states looked to enact and/or amend existing state data security laws this year. Seventeen states (AL, AZ, CO, DE, IL, IA, KY, LA, MD, MO, NE, NJ, OR, RI, SD, TN, and VA) introduced and six states (IL, MA, MI, NY, OH, and PA) carried over bills, totaling more than 40 data security bills active this legislative session. AL, AZ, CO, DE, LA, NE, OR, and SD enacted data breach legislation this year.

Below is a chart tracking data security legislation active in the states in the 2018 legislative sessions.

State	Status	Existing Law	Key Provisions
Alabama HB 410/ SB 318	SB 318: **ENACTED 3/27/2018.** HB 410: **BILL DIED.**	No	Creates the Alabama Data Breach Notification Act. Defines "breach of security or breach" as the unauthorized acquisition of data in electronic form containing sensitive personally identifying information. Acquisition occurring over a period of time committed by the same entity constitutes one breach. The term does not include any of the following: • Good faith acquisition of sensitive personally identifying information by an employee or agent of a covered entity, unless the information is used for a purpose unrelated to the business or subject to further unauthorized use.

State	Status	Existing Law	Key Provisions
			• The release of a public record not otherwise subject to confidentiality or nondisclosure requirements. • Any lawful investigative, protective, or intelligence activity of a law enforcement or intelligence agency of the state, or a political subdivision of the state. Defines "covered entity" as a person, sole proprietorship, partnership, government entity, corporation, nonprofit, trust, estate, cooperative association, or other business entity that acquires or uses sensitive personally identifying information. Defines "sensitive personally identifying information" as an individual's first name or first initial and last name in combination with one or more of the following: • A non-truncated SSN or tax ID; • A non-truncated driver's license number, state-issued ID card number, passport number, military ID number, or other unique ID number issued on a government document used to verify the identity of a specific individual; • A financial account number, including a bank account number, credit card number, or debit card number, in combination with any security code, access code, password, expiration date, or PIN, that is necessary to access the financial account or to conduct a transaction that will credit or debit the financial account; • Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; • An individual's health insurance policy number or subscriber ID number and any unique identifier used by a health insurer to identify the individual; • A user name or email address, in combination with a password or security question and answer that would permit access to an online account affiliated with the covered entity that is reasonably likely to contain or is used to obtain sensitive personally identifying information. The term does not include (1) information about an individual which has been lawfully made public by a federal, state, or local government record or a widely distributed media; or (2) information that is truncated, encrypted, secured, or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable, including encryption of the data, document, or device containing the sensitive personally identifying information, unless the covered entity knows or has reason to know that the encryption key or security credential that could render the

State	Status	Existing Law	Key Provisions
			personally identifying information readable useable has been breached together with the information. Defines "third-party agent" as an entity that has been contracted to maintain, store, process, or is otherwise permitted to access sensitive personally identifying information in connection with providing services to a covered entity. *Safeguarding information:* Requires each covered entity and third-party agent to implement and maintain reasonable security measures to protect sensitive personally identifying information against a breach of security. Reasonable security measures means security measures practicable for the covered entity to implement and maintain, including consideration of all of the following: • Designation of an employee or employees to coordinate the covered entity's security measures to protect against a breach of security. An owner or manager may designate him/herself. • Identification of internal and external risks of breach of security. • Adoption of appropriate information safeguards to address identified risks of a breach of security and assess the effectiveness of such safeguards. • Retention of service providers, if any, that are contractually required to maintain appropriate safeguards for sensitive personally identifying information. • Evaluation and adjustment of security measures to account for changes in circumstances affecting the security of sensitive personally identifying information. • Keeping the management of the covered entity appropriately informed of the overall status of its security measures. An assessment of a covered entity's security shall be based upon the entity's security measures as a whole and shall place an emphasis on data security failures that are multiple or systemic, including consideration of several factors including the size of the entity, the amount of sensitive personally identifying information and types of activities for which it was accessed, and the cost to implement and maintain security measures. Requires a covered entity after determining a breach has occurred to conduct a good faith and prompt investigation that includes an assessment of the nature and scope of the breach; identifying the information that was breached; and determining the harm.

State	Status	Existing Law	Key Provisions
			Notification: • Requires covered entities to provide notice of a breach to individuals affected. This shall be done as expeditiously as possible and without unreasonable delay. • Requires notice within 45 days of the covered entity's determination that a breach has occurred and is reasonably likely to cause substantial harm to the individuals to whom the information relates. • Notice may delayed if a federal or state law enforcement agency determines that notice would interfere with a criminal investigation or national security. • Requires notice to be made in writing or email and establishes notice content requirements. • Substitute notice may be provided if direct notice is not feasible due to (1) excessive costs of providing notice; (2) lack of sufficient contact information for individuals; and (3) affected individuals exceed 500,000 persons. • Substitute notice may be placed on the internet website of the covered entity or in print or broadcast media. Alternative notice may be used with the approval of the attorney general. • If the number of individuals a covered entity is required to notify exceeds 1,000, the entity shall provide written notice of the breach to the attorney general as expeditiously as possible without unreasonable delay. Notice shall be provided within 45 days of the covered entity's determination that a breach has occurred and is reasonably likely to cause substantial harm. • Establishes requirements for notice to the attorney general. • Requires notice to consumer reporting agencies if more than 1,000 individuals at a single time are affected. • Third-party agents experiencing the breach shall notify the covered entity as expeditiously as possible without unreasonable delay, but no later than 10 days following the determination of a breach or reason to believe a breach has occurred. Then the covered entity is required to provide notice of the breach consistent with notice requirements established.
Arizona	**ENACTED 4/11/2018.**	Yes	Amends current law definitions for "breach or security system breach"; "encrypted"; and

State	Status	Existing Law	Key Provisions
HB 2154			"personal information". Includes definitions for "unredacted" and "security incident." Amends current law to require a business that maintains, or licenses unencrypted or unredacted computerized data that includes personal information becomes aware of a security incident, to conduct a reasonable investigation to promptly determine whether there has been a security system breach. Investigations determining there was a breach, requires notice within 30 days after the determination of a breach. Requires notice in writing to the attorney general and individuals affected by the breach. If the breach requires notification to more than 1,000 state residents the person that owns or licenses the computerized data shall notify, promptly and without unreasonable delay, and subject to the needs of law enforcement, consumer reporting agencies that compile and maintain files on a nationwide basis. Amends current law replacing the term "breach of the security system" with "security system breach." Also includes "unredacted" anywhere "unencrypted" is mentioned. Notification is required to include at least the following: (1) the approximate date of the breach; (2) a brief description of the personal information included in the breach; (3) the number and addresses for the three largest consumer reporting agencies; and (4) the number, address, and website for the FTC or any federal agency that assists consumers with identity theft matters.
Colorado HB 1128	**ENACTED 5/29/2018.**	Yes	Amends current law: Includes provisions with respect to safeguarding Information: Requires a person who maintains, owns or licenses personal identifying information of an individual residing in Colorado to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal identifying information and the nature and size of the business and its operations. A person who uses a nonaffiliated third party as a service provider to perform services for the person and discloses personal identifying information about an individual residing in Colorado with the nonaffiliated third party shall require that the nonaffiliated third party

State	Status	Existing Law	Key Provisions
			implement and maintain reasonable security procedures and practices that are: (1) Appropriate to the nature of the personal identifying information disclosed to the nonaffiliated third party; and (2) Reasonably designed to help protect the personal identifying information from unauthorized access, use, modification, disclosure or destruction. Adds definitions for and amends definitions of the following terms: "commercial entity," "encrypted," "personal information," and "security breach." Requires notices to be sent within the most expedient time possible and without unreasonable delay but not later than 45 days from the date of the security breach. Notices must include, but need not be limited to, the following information: • the date, estimated date, or estimated date range of the security breach; • a description of the personal information that was acquired or reasonably believed to have been acquired as part of the security breach; • information that the resident can use to contact the individual or commercial entity that was breached to inquire about the security breach; • the toll-free numbers, addresses, and websites for consumer reporting agencies and the FTC; and • a statement that the resident can obtain information from the FTC and credit reporting agencies about fraud alerts and security freezes. The breach of encrypted or otherwise secured personal information must be disclosed if the confidential process, encryption key, or other means to decipher the secured information was also acquired in the security breach or was reasonably believed to have been acquired. An individual or commercial entity that is required to provide notice is prohibited from charging the cost of providing such notice to individuals. Also requires notice of security breaches to be provided to the attorney general as soon as practicable but not later than 7 days after discovery of the unauthorized acquisition of data if such acquisition affected or is reasonably believed to have affected 500 Colorado residents or more.

State	Status	Existing Law	Key Provisions
Delaware HB 465	**ENACTED 9/4/2018.**	Yes	Amends current law, making technical changes to substitute notice requirement postings to one or more websites.
Illinois SB 3007	**BILL DIED.**	Yes	Amends current law to add notice requirements of a security breach to the attorney general. Establishes requirements to be contained in the notice to the AG. Requires such notice to be made within 14 business days of the data collector's discovery of a breach or when it provides notice to the consumer, which ever is sooner. This requirement also applies to any data collector that maintains and stores data, but does not own the data.
Illinois HB 4367	**BILL DIED.**	Yes	Amends current law to require notification of a data security breach to be made by private entities within 14 days after discovery of the breach and by public entities in the most expedient time possible and without unreasonable delay.
Illinois HB 4174	**BILL DIED.**	Yes	Amends current law. Requires any data collector that owns or licenses personal information concerning an Illinois resident to notify the resident of any security breach of the system within 48 hours of discovery of the breach (rather than requiring notification in the most expedient time possible and without unreasonable delay).
Iowa HB 2423	**BILL DIED.**	Yes	Amends current law. • Amends the definition of "breach of security" to mean the unauthorized acquisition, or reasonable belief of unauthorized acquisition, of personal information maintained in computerized form by a person that compromises the security, confidentiality, or integrity of the personal information. • Amends the definition of "encryption" to include "accepted industry standards" to describe the algorithmic process of transforming data. • Adds to current exemptions from the law, a person who is subject to and complies with HIPAA and HITECH.

State	Status	Existing Law	Key Provisions
Iowa HSB 526	**BILL DIED.**	Yes	Amends current law: • The definition of "security breach" to mean the unauthorized acquisition or reasonable belief of unauthorized acquisition, of personal information maintained in any form, including but not limited to electronic or paper form, by a person that compromises the security, confidentiality, or integrity of the personal information. • The definition of "encryption" to include the use of a 180 bit or higher algorithmic process. • The definition of "personal information" as including financial account number, credit card number or debit card number. Also amends the definition of "personal information" to include medical information and health insurance information. • Amends current law to require any notice of a breach of security to be provided no later than 45 days after the discovery of such breach. Notification must also be provided to the attorney general within five business days after document a breach. • Requires written notice to the attorney general to include: ▪ A sample copy of any notification sent to consumers; ▪ The approximate number of consumers affected or potentially affected; ▪ A description of services offered to consumers affected or potentially affected by the breach and instructions as to how they may use such services; ▪ Information a contact within the attorney general's office for assistance; and ▪ The federal employer ID number.
Kentucky HB 188 and SB 33	**BILLS DIED.**	Yes	Adds definitions to current law for "personally identifiable information," and "security breach." Establishes requirements for consumer reporting agencies encryption of data and placing security freezes on accounts.
Louisiana SB 361	**ENACTED 5/20/2018.**	Yes	Amends current law: • Adds passport number and biometric data to the definition of personal information.

State	Status	Existing Law	Key Provisions
			• Any person that conducts business in the state or that owns or licenses computerized data that includes personal information, or agency that owns or licenses computerized data that includes personal information, shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information from unauthorized access, destruction, use, modification, or disclosure. • Any person that conducts business in the state or that owns or licenses computerized data that includes personal information, or any agency that owns or licenses computerized data that includes personal information shall take all reasonable steps to destroy or arrange for the destruction of the records within its custody or control containing personal information that is no longer to be retained by the personal or business by shredding, erasing, or otherwise modifying the personal information in the records to make it unreadable or undecipherable through any means. • Notification of a security breach shall be made not later than 45 days after the discovery of a breach.
Maryland HB 1584	**BILL DIED.**	Yes	Amends current law: • Entities that "maintain" computerized data are now also subject to the law. • If a business that incurred a breach is not the owner or licensee of the computerized data, the business may not charge the owner or licensee of the computerized data a fee for providing information that the owner or licensee needs to make a notification. • The owner or licensee of computerized data may not use information relative to the breach for purposes other than providing notification of the breach or protecting or securing personal information. • Notice of a breach may alternatively be done by conspicuously posting the notice on the website of the business, by notification to statewide media, or conspicuously posting notice at the business's place of business. Deletes provisions that allows alternative or substitute notice if the business demonstrates that the cost of providing notice would exceed $100,000 or 175,000 individuals. • After receiving notice of a breach from a business, requires the attorney general to post notice of the breach on the AG's website.

State	Status	Existing Law	Key Provisions
Massachusetts HB 2814/ SB 149	**BILLS DIED.**	Yes	Amends current law: • Does not make any person or agency that owns or licenses the data liable for damages from a security breach when: (1) the data owner or licensor is in compliance with state law; and (2) the security breach was not the result of intentional misconduct or the negligence of the data licensor, its agents, or employees. Permits any person who has been injured by a security breach to bring a civil action for actual damages, reasonable attorney's fees, and court costs. • Clarifies that remedies are cumulative and do not affect the availability of remedies under other law. • Establishes a commission on cybersecurity to assess the various cybersecurity threats across the state and to recommend corresponding legislative action, risk-management strategies, and response plans. Establishes commission membership and operations criteria. • Adds a definition of "biometric indicator", "encrypted", and "information security program." Amends the definition of "breach of security" and personal information." • Allows a substitute notice if the person or agency required to provide notice demonstrates that the cost of providing written notice will exceed $250,000, or that the affected class of Massachusetts residents to be notified exceeds 500,000 residents, or that the person or agency does not have sufficient contact information to provide notice. Requires substitute notice to consist of all of the following: (i) electronic mail notice, if the person or agency has electronic mail addresses for the members of the affected class of Massachusetts residents; (ii) clear and conspicuous posting of the notice on the home page of the person or agency if the person or agency maintains a website; and (iii) publication in or broadcast through media or medium that provides notice throughout the commonwealth. • The department of consumer affairs and business regulation may adopt regulations, from time to time, to revise the definition of "encrypted", as used in this chapter, to reflect applicable technological advancements. • The department of consumer affairs and business regulation shall adopt regulations relative to any person that owns or licenses personal information about a resident of the commonwealth. Such regulations shall require a person subject to this chapter to

State	Status	Existing Law	Key Provisions
			develop, implement, and maintain a comprehensive information security program that contains administrative, technical, and physical safeguards that are reasonably designed to (1) ensure the security and confidentiality of personal information of residents of the commonwealth, (2) protect against any anticipated threats or hazards to the security or integrity of such information; and (3) protect against unauthorized acquisition of such information that could result in substantial harm to the individuals to whom such information relates.
Massachusetts HB 1985/ SB 95	**BILLS DIED.**	Yes	Amends current law to include a definition of "biometric information" defined as any unique biological attribute or measurement that can be used to authenticate the identity of an individual, including but not limited to fingerprints, genetic information, iris or retina patters, facial characteristic, and hand geometry.
Massachusetts SB 149	**BILL DIED.**	Yes	Amends current law to: • Define "breach of security" as the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the commonwealth. A good faith but unauthorized acquisition of personal information by a person or agency, or employee or agent thereof, for the lawful purposes of such person or agency, is not a breach of security unless the personal information is used in an unauthorized manner or subject to further unauthorized disclosure. • Define "encrypted" as transformation of data through the use of a 128-bit or higher algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key, unless further defined by regulation of the department of consumer affairs and business regulation. • Notice shall include: (i) written notice; (ii) electronic notice, if notice provided is consistent with the provisions regarding electronic records and signatures pursuant to federal law; or (iii) substitute notice, if the person or agency required to provide notice demonstrates that the cost of providing written notice will exceed $250,000, or that the affected class of Massachusetts residents to be notified exceeds 500,000 residents, or that

State	Status	Existing Law	Key Provisions
			the person or agency does not have sufficient contact information to provide notice. • Defines "personal information" as a resident's first name and last name or first initial and last name in combination with any 1 or more of the following data elements that relate to such resident: (a) a SSN; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that "Personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public. • Allows "substitute notice" to consist of all of the following: (i) electronic mail notice, if the person or agency has electronic mail addresses for the members of the affected class of Massachusetts residents; (ii) clear and conspicuous posting of the notice on the home page of the person or agency if the person or agency maintains a website; and (iii) publication in or broadcast through media or medium that provides notice throughout the commonwealth. • The notice to be provided to the resident shall include, but not be limited to, the consumer's right to obtain a police report, how a consumer requests a security freeze and the necessary information to be provided when requesting the security freeze, and any fees required to be paid to any of the consumer reporting agencies. • No person or entity conducting business in Massachusetts that accepts an access device in connection with a transaction shall retain the card security code data, the PIN verification code number, or the full contents of any track of magnetic stripe data, subsequent to the authorization of the transaction or in the case of a PIN debit transaction, subsequent to 48 hours after authorization of the transaction. A person or entity is in violation of this section if its service provider retains such data subsequent to the authorization of the transaction or in the case of a PIN debit transaction, subsequent to 48 hours after authorization of the transaction. • Whenever there is a breach of the security of the system of a person or entity that has violated this section, or that person's or entity's service provider, that person or entity shall reimburse the financial institution that issued any access devices affected by the breach for the costs of reasonable actions undertaken by the financial institution as a result of the breach in order to protect the information of its cardholders or to continue to provide services to cardholders, including but not limited to, any cost incurred in

State	Status	Existing Law	Key Provisions
			connection with: (1) the cancellation or reissuance of any access device affected by the breach; (2) the closure of any deposit, transaction, share draft, or other accounts affected by the breach and any action to stop payments or block transactions with respect to the accounts; (3) the opening or reopening of any deposit, transaction, share draft, or other accounts affected by the breach; (4) any refund or credit made to a cardholder to cover the cost of any unauthorized transaction relating to the breach; and (5) the notification of cardholders affected by the breach. • This chapter does not relieve a person or agency from the duty to comply with requirements of any applicable general or special law or federal law regarding the protection and privacy of personal information; provided however, a person who maintains procedures for responding to a breach of security pursuant to federal laws, rules, regulations, guidance, or guidelines, is deemed to be in compliance with this chapter if the person notifies affected Massachusetts residents in accordance with the maintained or required procedures when a breach occurs; provided further that the person also notifies the attorney general and the director of the office of consumer affairs and business regulation of the breach as soon as practicable and without unreasonable delay following the breach. • The notice to be provided to the attorney general and the director of the office of consumer affairs and business regulation shall consist of, but not be limited to, any steps the person or agency has taken or plans to take relating to the breach pursuant to the applicable federal law, rule, regulation, guidance or guidelines; provided further that if said person or agency does not comply with applicable federal laws, rules, regulations, guidance or guidelines, then it shall be subject to the provisions of this chapter.
Michigan HB 4983	Carried over from 2017 session. Introduced 9/19/2017. Session is in recess.	Yes	Amends current law: • Requires notices to individuals who are the subject of a security breach to provide the date of the breach and describe the breach in general terms. • Requires after a person or agency provides notice, the person or agency to post the notice in a prominent and conspicuous place on its website that is fully accessible to its customers and the public. Also requires the website to include information about all of

State	Status	Existing Law	Key Provisions
			its security breaches sorted chronologically. • Requires all the security breach information a person or agency posts to its website to be provided to the attorney general.
Missouri HB 2264	**BILL DIED.**	Yes	▪ Amends current law definitions for "security breach," "health insurance information," "medical information," "owns or licenses," "person," and "personal information." ▪ Amends current law to require notification to consumers within 48 hours of the discovery of a breach (rather than "without unreasonable delay").
Nebraska LB 757	**ENACTED 2/28/2018.**	Yes	Amends current law. Requires an individual or commercial entity that owns, licenses, or maintains data that includes personal information about a resident of Nebraska to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal information owned, licensed, or maintained and the nature and size of the business and its operations, including safeguards that protect the personal information when the individual or commercial entity disposes of the personal information. Deems compliance with this provision if the individual or entity complies with GLBA. Requires individuals and commercial entities that disclose personal information to a nonaffiliated third party service provider shall require by contract that the third party implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal information disclosed to the nonaffiliated third party; and are reasonably designed to help protect the personal information from unauthorized access, acquisition, destruction, use, modification, or disclosure.
New Jersey AB 3541	Introduced 3/5/2018.	Yes	Amends current law to require notice to a customer of a security breach to be made without unreasonable delay, not to exceed five business days. Notice is not required if, after an appropriate investigation by the business or public entity and consultation with relevant federal, state, or local agencies responsible for law enforcement, the business or public entity establishes that misuse of the information is not reasonably possible.

State	Status	Existing Law	Key Provisions
New Jersey AB 1766/ SB 2692	SB 1766: Introduced 1/9/2018 and referred to House Homeland Security and State Preparedness Committee for 1st reading. SB 2692: Introduced and referred to Senate Law and Public Safety Committee 6/11/2018.	Yes	Requires any person, corporation, association, partnership or other legal entity that owns or licenses personal information about a resident of New Jersey to develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are necessary to protect the personal information.
New Jersey SB 52/ AB 3245	SB 52: Introduced 1/9/2018 and referred to Senate Commerce Committee for 1st reading. Reported Senate Commerce Committee amendments – 2nd reading 5/10/2018. Passed the Senate 6/25/2018. Referred to Assembly Financial Institutions and Insurance Committee. AB3245: Introduced 2/12/2018 and	Yes	Adds user names, email addresses, or any other account holder identifying information, in combination with any password or security question and answer that would permit access to an online account, to the list of breaches requiring disclosure. Notification of a breach provides a consumer with the opportunity to quickly change online account information to prevent outside access to the account and puts a consumer on notice to monitor for potential identity theft.

State	Status	Existing Law	Key Provisions
	referred to Assembly Financial Institutions and Insurance Committee.		
New Jersey SB 1524	Introduced and referred to Senate Commerce Committee 2/5/2018.	Yes	Amends current law to require any disclosure of a security breach to a customer shall be done without unreasonable delay, not to exceed five business days. Disclosure of a breach of security to a customer shall not be required if, after appropriate investigation by the business or public entity and consultation with relevant state, federal and local agencies responsible for law enforcement that the misuse of the information is not reasonably possible.
New York AB 8884	Referred to Consumer Affairs and Protection 1/4/2018. Session is in recess.	Yes	Amends current law. • Definition of "personal information" is amended to include biometric information, user name or email address in combination with a password or security question, and any HIPAA related information. • In determining whether information has been accessed, or is reasonably believed to have been accessed, by an unauthorized person or a person without valid authorization, such business may consider, among other factors, indications that the information was viewed, communicated with, used, or altered by a person without valid authorization or by an unauthorized person. • Substitute notice of a security breach may be provided via email, except if the breached information includes an email address in combination with a password or security question and answer that would permit access to the online account. Adds to current law to require any person or business that owns or licenses computerized data which includes private information of a resident of New York to develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information including but not limited to, disposal of data.

State	Status	Existing Law	Key Provisions
			A person or business is deemed compliant if it has a data security program that has: (1) Administrative safeguards such as the following, in which the person or business, a. Designates one or more employees to coordinate the security program; b. Identifies reasonably foreseeable internal and external risks; c. Assesses the sufficiency of safeguards in place to control the identified risks; d. Trains and manages employees in the security program practices and procedures; e. Selects service providers capable of maintaining appropriate safeguards, and requires those safeguards by contract; and f. Adjusts the security program considering business changes or new circumstances; and (2) Technical safeguards such as the following, in which the person or business: a. Assesses risks in network and software design; b. Assesses risks in information processing, transmission and storage; c. Detects, prevents and responds to attacks or system failures; and d. Regularly tests and monitors the effectiveness of key controls, systems and procedures; and (3) Physical safeguards such as the following, in which the person or business: a. Assesses risks of information storage and disposal; b. Detects, prevents and responds to intrusions; c. Protects against unauthorized access to or use of private information during or after the collection, transportation and destruction or disposal of the information; and d. Disposes of private information within a reasonable amount of time after it no longer needed for business purposes by erasing electronic media so that the information cannot be read or reconstructed.
New York AB 180	Carried over from 2017 session. Introduced 1/4/2017 and referred to Assembly Committee on Consumer	Yes	Amends current law to require 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 within five days of the 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.

State	Status	Existing Law	Key Provisions
	Affairs and Protection. Session is in recess.		Deletes provisions stating that the disclosure be made in the most expedient time possible without unreasonable delay.
New York AB 7167	Carried over from 2017 session. Introduced 4/12/2017. Reported and referred to Codes 4/25/2017. Reported and referred to Assembly Ways and Means Committee 5/16/2017. Reported and referred to Assembly Rules 6/19/2017. Rules report cal. 497 6/19/2017 and ordered to third reading in Rules. Session is in recess.	Yes	Amends current law: • Amends the definition of "private information" to include biometric information. • Disclosure of a breach of the security system is required when private information is acquired without a valid authorization or by an unauthorized person. • Amends requirements with respect to email notices of a security breach. • Allows the department of state to receive complaints pursuant to security breach violations and to make referrals as appropriate and in coordination with the attorney general re: regularly updating and making publicly available information relating to how to respond to a security breach.
New York AB 7232	Carried over from 2017 session. Introduced 4/12/2017. Amended and recommitted	Yes	Amends current law with respect to reasonable delay in notification. Reasonable delay shall not exceed 45 days, unless the person or business seeking additional time demonstrates to the attorney general that additional time is reasonably necessary to determine the scope of the breach of the security system, prevent further disclosures, conduct the risk assessment, and restore the reasonable integrity of the security system. If the attorney general determines that additional delay is necessary, the agency may extend the time period for notification for

State	Status	Existing Law	Key Provisions
	to Assembly Committee on Consumer Affairs and Protection 5/24/2017. Reported and referred to Codes 6/5/2017. Session is in recess.		additional periods of up to 45 days each. Any disclosure shall be made without unreasonable dely. Deletes current law requirement of "in the most expedient time possible."
New York AB 8756/ SB 6933	Carried over from 2017 session. AB 8756: Introduced 10/31/2017 and referred to House Consumer Affairs and Protection Committee. SB 6933: Introduced 11/1/2017 and referred to Senate Rules. Session is in recess.	Yes	Amends current law: • Amends the definition of "private information" to mean either: (1) personal information consisting of any information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted, or encrypted with an encryption key that has also been access or acquired (a) SSN; (b) driver's license number or non-driver ID card number; (c) account number, credit or debit card number, in combination with any required security code, access code password or other information that would permit access to an individual's financial account; (d) account number, credit or debit card number, if circumstances exist wherein such number could be used to access an individual's financial account without additional identifying information, security code, access code or password; or (e) biometric information, meaning data generated by automatic measurements of an individual's physical characteristics, which are used to authenticate the individual's identity; (2) a user name or email address in combination with a password or security question and answer that would permit access to an online account; or (3) any unsecured protected health information held by a "covered entity" as defined in HIPAA. • Amends the definition of "breach of the security system" to using the term "private information" instead of "personal information. Also adds that in determining whether information has been accesses, or is reasonably believed to have been accessed, by an unauthorized person or a person without valid authorization, a business may

State	Status	Existing Law	Key Provisions
			consider, among other factors, indications that the information was viewed, communicated with, used, or altered by a person without valid authorization or by an unauthorized person. • Amends current law to allow substitute notice that includes emails except if the breached information contained an email address in combination with a password or security question and answer that would permit access to an online account. • Imposes data security protections on "complaint regulated entities" which means any person or business that is subject to GLBA, HIPAA, HITEC, and New York state privacy laws." • Requires any person or business that owns or licenses computerized data which includes private information of a resident of New York to develop, implement and maintain reasonable safeguards to protect the security, confidentiality, and integrity of the private information including, but not limited to, disposal of data. • A person or business is deemed compliant if they are a "certified complaint entity" in compliance with GLBA, HIPAA, HITEC and has implemented a data security program that includes: o administrative safeguards including the designation of one or more employees to coordinate the security program; identifying reasonably foreseeable internal and external risks; assessment of the sufficiency of safeguards in place to control the identified risks; and training and management of employees in security program practices and procedures; o technical safeguards including assessment of risks in network and software design, information processing, transmission, and storage; detection, prevention, and response to attacks of system failures; and o physical safeguards including disposing of private information.
New York SB 1104	Carried over from 2017 session. Introduced 1/6/2017 and referred to Senate Committee on Consumer Protection.	Yes	Amends current law to require 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 without unreasonable delay, consistent with the legitimate needs of law enforcement. Reasonable delay shall not exceed 45 days, unless the

State	Status	Existing Law	Key Provisions
	First report Cal.250 2/14/2017. Second report Cal. 2/28/2017. Advanced to third reading 3/1/2017. Committed to Rules Committee 6/21/2017. Session is in recess.		person or business seeking additional time demonstrates to the attorney general that additional time is reasonably necessary to determine the scope of the breach of the security system, prevent further disclosures, conduct the risk assessment, and restore the reasonable integrity of the security system. If the attorney general determines that additional delay is necessary, the agency may extend the time period for notification for additional periods of up to 45 days each. Any such extension shall be provided in writing.
New York SB 5601	Carried over from 2017 session. Introduced and referred to Committee on Consumer Protection 4/19/2017. First reading 4/25/2017. Second reading 4/26/2017. Third reading 5/1/2017. Committed to Rules 6/21/2017. Session is in recess.	Yes	Amends the definition of "private information" to include biometric information. Amends the definition "breach of the security of the system" to replace "personal information" with "private information." Also adds "a person without valid authorization" within the definition. Amends substitute notice provisions to consist e-mail notice when such business has an e-mail address for the subject persons, provided the breached information does not include an e-mail address in combination with a password or security question and answer that would permit access to the online account, in which case, the person or business shall not comply with this section by providing notice to that e-mail account, but shall be by clear and conspicuous notice delivered to the consumer online when the consumer is connected to the online account from an internet protocol address or from an online location which the person or business knows the consumer customarily accesses the online account; Amends penalties to $20 per instance instead of $10 and not to exceed $250,000 rather than $150,000.

State	Status	Existing Law	Key Provisions
			Regardless of the method by which notice is provided, such notice shall include contact information for the person or business making the notification, the telephone numbers and websites of the relevant state and federal agencies that provide information regarding security breach response and identity theft prevention and protection information, and a description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization or by an unauthorized person, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so acquired.
New York SB 8641	Introduced 5/10/2018 and referred to Senate Committee on Consumer Protection. Session is in recess.	Yes	Creates a private right of action for the breach of a consumer's identifying information. A user of information, in possession of a consumer's identifying information when such identifying information is impermissibly obtained by an unauthorized third party, is liable to the consumer in an amount equal to: (1) $10,000; (2) any actual damages sustained by the consumer as a result of such breach of identifying information; and (3) in the case of any successful action to enforce any liability the costs of the action together with reasonable attorney fees as determined by the court.
Ohio SB 220	Introduced 10/17/2017. Carried over from 2017 session. Referred to and passed Senate Oversight Committee 5/16/2018. Referred to House Government Accountability and Oversight Committee 6/5/2018.	Yes	Establishes a legal safe harbor to as an affirmative defense to a cause of action that alleges the failure to implement reasonable information security controls resulted in a data breach. The safe harbor shall apply to all covered entities that implement a cybersecurity program that complies with the Framework for Improving Critical Infrastructure Cybersecurity developed by the National Institute of Standards and Technology, or other industry recognized data security framework.

State	Status	Existing Law	Key Provisions
	Session is in recess.		
Oregon HB 4147/SB 1551	SB 1551: **ENACTED 4/23/2018.** HB 4147: **BILL DIED.**	Yes	Amends current law: • A person required to give notice of a security breach shall do so in the most expeditious manner possible, without unreasonable delay, consistent with any measures that are necessary to determine sufficient contact information for the recipient of notice, determine the scope of the breach of security and restore the reasonable integrity, security and confidentiality of the personal information, but in no event more than 45 days from the time the person discovers or receives notice of the security breach. A person that owns, maintains or otherwise possesses data that includes a consumer's personal information that the person uses in the course of the person's business, vocation, occupation, or volunteer activities shall develop, implement and maintain reasonable safeguards to protect the security, confidentiality, and integrity of the personal information, including safeguards that protect the personal information when the person disposes of the personal information. Requires the implementation of an information security program that includes: (1) Administrative safeguards such as: (a) designated one or more employees to coordinate the security program, identifying reasonably foreseeable internal and external risks with reasonable regularity; (b) assessing whether existing safeguards adequately control the identified risks; (c) regularly training and maintaining employees in security program practices and procedures; (d) selecting service providers that are capable of maintaining appropriate safeguards, procedures and protocols, and requiring the service providers by contract to maintain the safeguards, procedures and protocols; (e) Adjusting the security program in light of business changes, potential threats or new circumstances; (f) Communicating with and training employees regarding potential

State	Status	Existing Law	Key Provisions
			threats and business impacts of potential threats; (g) Implementing and maintaining a patch management program in which recommended software and hardware patches are applied within a reasonable time; and (h) Performing user access reviews with reasonable regularity to monitor and verify the appropriateness of users' access to systems and information. (2) Technical safeguards such as: (a) Assessing risks in network and software design and taking reasonable and timely action to address weaknesses or vulnerabilities; (b) Assessing risks in information collection, processing, transmission, and storage; (c) Monitoring, detecting, preventing and responding to attacks or system failures; (d) Testing and monitoring regularly the effectiveness of key controls, systems and procedures and implementing remedial actions for identified weaknesses or deficiencies; and (e) Ensuring that personal information of customers is properly segregated and accessible only to authorized users. (3) Physical safeguards such as: (a) Assessing known and potential risks of information collection, storage, usage, retention, access and disposal, followed by implementation of action plans to remedy or mitigate identified risks; (b) Monitoring, detecting, preventing, isolating and responding to intrusions within a reasonable timeframe; (c) Protecting against unauthorized access to or use of personal information during or after collecting, using, storing, accessing, transporting, destroying or disposing of the personal information; and (d) Disposing of personal information, including personal information held offsite, after the person no longer needs the personal information for business purposes or as required by local, state, or federal law for record retention.
Pennsylvania	Carried over from 2017	Yes	Amends current law to establish notification of a security breach by a state agency.

State	Status	Existing Law	Key Provisions
HB 848	session. Introduced and referred to Judiciary 3/13/2017.		Establishes storage policies the state must undertake to ensure the security of personally identifiable information.
Pennsylvania HB 33	Carried over from 2017 session. Introduced and referred to House Commerce Committee 1/23/2017.	Yes	Amends current law to require notice of a breach to go to the Attorney General and the Cybersecurity Coordinator. Amends current law deleting the requirement that notice be provided "without unreasonable delay" and replaces it with "no later than 30 days after discovery of the breach."
Pennsylvania HB 36	Carried over from 2017 session. Introduced and referred to House Commerce Committee 1/23/2017.	Yes	Amends current law definition of "personal information" to include: ▪ identification numbers, such as: SSN; driver's license number; state ID card number issued in lieu of a driver's license; passport number; taxpayer ID number; patient ID number; insurance member number; and employee ID number; ▪ maiden names, mother's maiden name, and an alias; ▪ electronic identifiers or routing code, in combination with any required security code, access code, or password that would permit access to an individual's financial account; ▪ electronic account information, such as account name or user name; ▪ internet protocol (IP) or Media Access Control (MAC) address or other host-specific persistent static identifier that consistently links to a particular individual or small, well-defined group of individuals; ▪ biometric data, such as genetic information, a fingerprint, facial scan, retina or iris image, voice signature, x-ray image or other unique physical representation or digital representation of biometric data; ▪ date of birth; ▪ place of birth; ▪ insurance, employment, or education information; ▪ vehicle information;

State	Status	Existing Law	Key Provisions
			▪ contact information e.g., phone number, address, or email; or ▪ digitized or other electronic signature.
Pennsylvania HB 1846	Carried over from 2017 session. Introduced 10/13/17. Tabled 10/18/2017. Removed from table 1/2/2018. Recommitted to House Appropriations Committee 3/12/2018. Passed House Appropriations Committee 3/13/2018. Passed House 3/13/2018. Referred to Senate Communications and Technology Committee 3/16/2018.	Yes	Amends the definition of "breach of the security of the system" to the "loss, unauthorized access, acquisition or use of unencrypted data, encrypted data, the confidential process or key that is capable of compromising the security of confidentiality of personal information maintained by the entity as part of the database or personal information regarding multiple individuals. Good faith acquisition of personal information by an employee or agent of the entity for the purposes of the entity is not a breach of the security of the system if the personal information is not used for a purpose other than the lawful purpose of the entity and is not subject to further unauthorized disclosure." Adds a definition of "health insurance information" meaning "an individual's health insurance policy number or subscriber identification number, a unique identifier used by a health insurer to identify the individual or information in an individual's application and claims history, including appeal records." Adds a definition of "medical information" meaning "information regarding an individual's medical history, mental or physical condition or medical treatment or diagnosis by a health care professional." Amends the definition of "personal information" to "information that is under the control of an individual, is not otherwise generally available to the public through lawful means and is linked or linkable by the person to a specific individual or linked to a device that is associated with or routinely used by a specific individual, including: • An individual's first name or first initial and last name in combination with and linked to any one or more of the following data elements when the data elements are not encrypted or redacted: ▪ SSN; ▪Driver's license number or state ID card number issued in lieu of a driver's license; ▪Financial account number, credit or debit card number, in combination with any required security code, access code or password that would permit access

State	Status	Existing Law	Key Provisions
			to an individual's financial account. • Any of the following for an individual: ▪A government-issued ID number, including a tax ID and passport number; ▪A postal address; ▪An email address; ▪A phone or fax number; ▪A debit or credit card number; ▪Medical information; ▪Health insurance information; ▪A biometric identifier, including voice or fingerprint; ▪A unique persistent identifier, including a security or access code; ▪A unique identifier or other uniquely assigned or descriptive information about a personal computing or communication device; ▪Information that is collected, created, processed, used, disclosed, stored or otherwise maintained and linked or linkable by the person to any of the information enumerated under this paragraph. Amends current law to require notice to residents be in plain language and include: ▪ The ate, estimated date or date range of the breach of the security system; ▪ Whether the notification was delayed as a result of a law enforcement investigation; ▪ A list of types of information that were or are believed to have been subject to the breach of the security of the system; ▪ A general description of the breach of the security system; ▪ A toll-free number and addresses or consumer reporting agencies if the breach exposed a SSN or ID card number; and ▪ The name and contact information of the reporting agency that was notified. Entities providing may also include information about what the entity has done to protect affected individuals and offer advice on what steps affected individuals may take to protect their information and what steps the individual whose information has been breached may take to protect himself or herself. Requires notice to be made within 30 days of learning of the breach.

State	Status	Existing Law	Key Provisions
			Requires notice to the attorney general of a breach. Requires notice to the attorney general to include: ▪ The nature of the breach; ▪ The number of residents affected by the breach; ▪ Steps taken by the entity relating to the breach. Requires notice to the bureau of insurance without unreasonable delay, of the timing, distribution, and number of notices and any other information as required by the bureau. If an entity does not have a federal or state notification rule, regulation, procedure, or guideline in effect, the entity must also comply with this Act. <u>Safeguarding Personal Information:</u> An entity in possession of personal information of another person shall safeguard the data, computer files or documents containing the information from misuse by third parties and shall destroy, erase or make unreadable such data, computer files or documents prior to disposal. The entity shall develop a policy to govern the proper storage of data which includes personally identifiable information. The policy shall address identifying, collecting, maintaining, displaying and transferring personally identifiable information, using personally identifiable information in test environments remediating personally identifiable information stored on legacy systems and other relevant issues. A goal of the policy shall be to reduce the risk of future breaches of security of the system. An entity that collects personal information in the course of business shall create a privacy protection policy, which shall be published or publicly displayed, including posting on web page. The policy shall protect the confidentiality of the personal information, prohibit unlawful disclosure of personal information and limit access to personal information. When disposing of records, each entity shall meet the following minimum standards for proper disposal of records containing personal information: • Paper records continuing personal information shall be either redacted, burned,

State	Status	Existing Law	Key Provisions
			pulverized or shredded so that personal data cannot practicably be read or reconstructed; • Electronic records and other non-paper records containing personal information shall be destroyed or erased so that personal information cannot practicably be read or reconstructed. An entity disposing of personal information may contract with a third party to dispose of personal information in accordance with this section. A third party hired to dispose of material containing personal information shall implement and monitor compliance with policies and procedures that prohibit unauthorized access to or acquisition of or use of personal information during the collection, transportation and disposal of personal information. The following are considered unfair methods of competition and unfair or deceptive acts or practices by an entity that collects or possesses personal information: • Failing to create a storage policy as described; • Failing to create, publish or publicly display or comply with a privacy protection as described; • Failing to dispose of records in a manner described; • Failing to provide consumers with opt-out consent prior to the entity using, disclosing or permitting a third party to have access to personal information of consumers or failing to provide consumer with a means to withdraw a previous consent; • Refusing to provide service to consumers who exercise their right to opt out of an entity using, disclosing or permitting a third party from having access to their personal information; or • Failing to reasonably safeguard or protect personal information, maintained by an entity or vendor, from a breach of the security of the system.
Pennsylvania SB 308	Carried over from 2017 session. Introduced 2/15/2017 and	Yes	Amends current law: • Creates a definition for "health insurance information" – defined as an individual's health insurance policy number or subscriber identification number or any

State	Status	Existing Law	Key Provisions
	referred to Senate Communications and Technology Committee.		medical information in an individual's insurance application and claims history, including any appeals records. • Creates a definition for "medical information" – defined as any individually identifiable information contained in or derived from the individual's current or historical record of medical necessity or medical treatment or diagnosis created by a health care professional. • Establishes electronic notification requirements. In the case of a breach of the security of the system involving personal information for a username or email address in combination with a password or security question and answer that would permit access to an online account, the person or business may comply by providing the security breach notification in electronic or other form that directs the person whose personal information has been breached to promptly change the person's password and security question or answer, as applicable, or to take other steps appropriate to protect the online account with the person or business and all other online accounts for which the person whose personal information has been breached uses the same username or email address and password or security question or answer. • Requires employees and contractors of the state to, while working with personal information on behalf of the state or otherwise conducting official business on behalf of the state, to utilize encryption to protect the transmission of personal information over the Internet from being viewed or modified by a third party. • Requires the governor's Office of Administration to develop and maintain a policy to govern the proper encryption and transmission by state agencies under the governor's jurisdiction of data which includes personal information. • Any entity or business association in compliance with the privacy and security standards for protection of electronic health information established under HIPAA and HITECH, shall be deemed to be in compliance with the provisions of this Act.
Rhode Island HB 7387	**BILL DIED.**	Yes	Defines "breach of the security system" 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 causes, or the individual or entity reasonably has caused or will cause identity theft or other fraud to any resident of the state. Good faith acquisition of personal information by an employee or agent

State	Status	Existing Law	Key Provisions
			of an individual or entity for the purposes of the individual or the entity is not a breach of the security system, provided that their personal information is not used for a purpose other than a lawful purpose of the individual or entity or subject to further unauthorized disclosure. Defines "personal information" as the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of this state, when the data elements are neither encrypted nor redacted: (1) SSN; (2) driver's license number or state ID card; (3) financial account number or credit or debit card number in combination with any required security code, access code or password that would permit access to a resident's financial accounts. An individual or entity that owns or licenses computerized data that includes personal information shall disclose any breach of the security system following discovery or notification of the breach to any resident 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. Requires disclosure to be made without unreasonable delay. 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 as soon as practicable following discovery, if the personal information was or the entity reasonably believes was accessed and acquired by an unauthorized person. Notice means: (i) written notice to the postal address in regards to the individual or entity; (ii) phone notice; (iii) electronic notice; or (iv) substitute notice if the individual or the entity required to provide notice demonstrated that the cost of providing notice will exceed 50,000 or that the affected class of residents to be notified exceeds 100,000 persons, or that the individual or the entity does not have sufficient contact information or consent to provide notice. Substitute notice may be provided via email if the individual or entity has email addresses for the members of the class of residents; by posting on the website of the individual or the entity

State	Status	Existing Law	Key Provisions
			if the individual or the commercial entity maintains a website; and via major statewide media. Notice may be delayed 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. An entity that maintains its own notification procedures as part of an information privacy or security policy for the treatment of personal information and that are consistent with the timing requirements are deemed to be in compliance with the notification requirements of this chapter if it notifies residents consistent with its procedures in case of a security breach. Also deems compliance if the individual or entity is compliant with federal requirements.
Rhode Island HB 7789/ SB 2497	**BILLS DIED.**	Yes	Amends current law replacing it with the NAIC data security model act.
South Dakota SB 62	**ENACTED 3/26/2018.**	Yes	Defines "breach of system security" as the unauthorized acquisition of unencrypted computerized data or encrypted computerized data and the encryption kay by any person that materially compromises the security, confidentiality, or integrity of personal or protected information maintained by the information holder. The term does not include the good faith acquisition of personal or protected information by an employer or agent of the information holder for the purposes of the information holder if the personal or protected information is not used or subject to further unauthorized disclosure. Defines "personal information" as a person's first name or first initial and last name, in combination with any one or more of the following data elements: (1) SSN; (2) driver license number or other unique identification number created or collected by a government body; (3) account, credit card, or debit card number, in combination with any required security code, access code, password, routing number, PIN, or any additional information that would permit access to a person's financial account; (4) health information; (5) an ID number assigned to a person's employer in combination with any required security code, access code, password, or biometric data generated from measurements or analysis of human body characteristics for

State	Status	Existing Law	Key Provisions
			authentication purposes. Defines "protected information" as (1) a user name or email address, in combination with a password, security question answer, or other information that permits access to an online account; and (2) account number or credit or debit card number, in combination with any required security code, access code, or password that permits access to a person's financial account. Following the discovery by or notification to an information holder of a breach of system security an information holder shall disclose the breach of system security to any resident of this state whose personal or protected information was, or is reasonably believed to have been, acquired by an unauthorized person. A disclosure shall be made not later than 60 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. An information holder is not required to make a disclosure if, 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. The information holder shall document the determination under this section in writing and maintain the documentation for not less than three years. Any information holder that experiences a breach of system security shall disclose to the attorney general by mail or electronic mail any breach of system security that exceeds 250 residents of the state. A notification required may be delayed if a law enforcement A disclosure may be provided by: (1) Written notice; (2) Electronic notice, if the electronic notice is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 in effect as of January 1, 2018, or if the information holder's primary method of communication with the resident of this state has been by electronic means; or

State	Status	Existing Law	Key Provisions
			(3) Substitute notice, if the information holder demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars, that the affected class of persons to be notified exceeds five hundred thousand persons, or that the information holder does not have sufficient contact information and the notice consists of each of the following: (a) Email notice, if the information holder has an email address for the subject persons; (b) Conspicuous posting of the notice on the information holder's website, if the information holder maintains a website page; and (c) Notification to statewide media. If an information holder discovers circumstances that require notification regarding more than 250,000 persons at one time, the information holder shall also notify, without unreasonable delay, all consumer reporting agencies, in effect as of January 1, 2018, and any other credit bureau or agency that compiles and maintains files on consumers on a nationwide basis, of the timing, distribution, and content of the notice. Notwithstanding any other provisions in this Act, any information holder that is regulated by federal law or regulation, including HIPAA or GLBA and that maintains procedures for a breach of system security pursuant to the laws, rules, regulations, guidance, or guidelines established by its primary or functional federal regulator is deemed to be in compliance with this chapter if the information holder notifies affected South Dakota residents in accordance with the provisions of the applicable federal law.
Tennessee HB 2508/SB 2536	**BILLS DIED.**	Yes	Amends current law: • Adds to the definition of "determination of a breach of system security" the point in time at which an information holder has sufficient information to conclude that a breach of system security occurred. • Adds to the definition of "personal information" medical information including mental and physical medical history, mental and physical treatment by a healthcare professional, diagnosis of mental or physical condition by a healthcare professional, or DNA profile; and health insurance information, including health insurance policy numbers, subscriber identification numbers, or any other unique identifiers used by a health insurer to identify an individual, or any medical information in an individual's health insurance application

State	Status	Existing Law	Key Provisions
			and claims history, including any appeals records. • Following determination of a breach of system security or following notification of a breach of system security by a third-party information holder, the information holder that owns the personal information at issue shall disclose the breach of system security within 45 days to any resident of this state whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person. When an information holder required to notify residents of this state of a breach of system security could not, through reasonable diligence, determine within 45 days that the personal information of certain residents of this state was included in a breach, the information holder must provide the notice required to such residents as soon as is practicable after it is determined that the personal information of those residents was included in a breach of system security, unless the information holder provides or has provided substitute notice in accordance with this section. • Any person whose personal information is owned, licensed, or maintained by an information holder that is not an agency of the state or any political subdivision of the state and who is injured by a violation of this section may institute a civil action to recover damages and to enjoin the information holder from further actions. • An information holder required to issue a notice disclosing a breach of system security, pursuant to this section, to more than 500 residents of this state shall immediately notify the attorney general of the breach and shall submit to the attorney general a sample copy of the breach notification concurrent with notifying such residents. Adds to current law - All information holders shall implement and maintain reasonable procedures and practices, commensurate with industry standards and with the size and complexity of the information, to prevent the unauthorized acquisition, use, modification, disclosure, or destruction of personal information collected or maintained in the regular course of business, including appropriate corrective action.
Virginia HB 679	**BILL DIED.**	Yes	Amends current law to state that "unreasonable delay" means a period not to exceed 30 days.