THE COUNCIL
The Council of Insurance Agents & Brokers

Steptoe

*UPDATED January 10, 2022*

# *Data Breach Notification Survey*

## INTRODUCTION

Forty-eight states and the District of Columbia have enacted laws imposing notification obligations on private or governmental entities in the event of a breach involving personally identifiable information.

The Data Breach Notification survey is designed to assist Council members in determining which states impose notification obligations on relevant parties following a breach event and provide information regarding those state laws. In particular, the survey documents each law's:

- Application to certain entities (i.e., businesses, data brokers, government entities, etc.);
- Coverage of certain data (i.e., name, social security number, account numbers, etc.);
- Classification of a breach;
- Notification requirements (i.e., when notice must be given, whether notice can be delayed, how notice must be given, etc.);
- Applicable exemptions; and
- Enforcement mechanisms.

Additionally, the survey contains insurance and broker-specific content, in the event actions are taken by the states' insurance regulators.

The below survey outlines the varying state approaches to insurance consultant licensure and regulation via a comparison of existing statutory text, associated regulatory provisions, and interpretive administrative guidance with respect to these specific provisions.

## QUICK LINKS BY STATE



## NEWLY INCLUDED UPDATES*

N/A

* We envision this survey to be an evergreen document. Any relevant updates—whether through legislative or administrative action—are included in this section and in ***bold and italicized blue text*** throughout the survey. We ask, therefore, that you continuously review the document for updates to any statutes, regulations, bulletins, or other guidance documents. That said, if you see laws enacted, regulations finalized, bulletins issued, or enforcement actions undertaken that are not reflected in this survey, please let us know.

| State | Covered Entities and Data | Method and Timing of Notice | Substitute Notice | Exceptions | Other |
|---|---|---|---|---|---|
| ***Alabama***<br><br>ALA. CODE §§ 8-38-1 et seq. | Applies to any business entity that acquires or uses ***sensitive personally identifiable information***, including a resident's first or last name plus:<br>• SSN/TIN<br>• Driver's license number, passport number, military ID number, etc.<br>• Financial account number plus a security code (e.g., debit card number and PIN).<br>• Information regarding medical history, mental/physical condition, etc.<br>• Health insurance policy number or any other identifier used by an insurer to identify the individual.<br>• User name/email plus password.<br><br>Does not include information that has lawfully been made public or that is truncated, encrypted, secured, deidentified, etc. | Requires notice in writing to affected individuals within 45 days of the determination that a breach has occurred and is reasonably likely to cause substantial harm to affected individuals.<br><br>If the breach requires notification of more than 1,000 affected individuals, requires notice to:<br>• The Attorney General within 45 days of the determination that a breach has occurred and is reasonably likely to cause substantial harm to affected individuals; and<br>• Consumer reporting agencies in accordance with federal law.<br><br>If a third-party (i.e., a "third party agent") experiences a breach, requires notification of the affected entity within 10 days of a determination of the breach or reason to believe the breach occurred. | In limited circumstances (i.e., if the cost of providing notice exceeds $500,000, the affected class of Alabama residents exceeds 100,000, or the entity does not have sufficient contact information), permits notice via a conspicuous notice on the entity's website and notice in print and broadcast media where the affected individuals reside. | Exempts or deems compliant certain entities from the breach notification requirements, including:<br>• Entities subject to federal requirements on data breach notification (but still requires notice to Attorney General when applicable)<br>• Entities with notification procedures that are at least as thorough as these the timing requirements in the broad data breach notification law. | ***Insurance-Specific Standards***. Adopts the NAIC Data Security Model Law.<br><br>***Penalties***. Provides that a violation is an unlawful trade practice and a knowing violation may result in civil penalties up to $500,000 per breach (provided it does not exceed $5,000 per day for each day that the entity fails to give notice).<br><br>***Private Right of Action***. Provides that a violation does not establish a private cause of action. |
| ***Alaska*** | Applies to any person "doing business" or business entity with more than 10 employees | Requires notice via written document or electronic means to each state resident whose | In limited circumstances (i.e., if the cost of providing | N/A | ***Waivers***. Renders waivers void/ unenforceable. |

| State | Covered Entities and Data | Method and Timing of Notice | Substitute Notice | Exceptions | Other |
|---|---|---|---|---|---|
| ALASKA STAT. ANN. §§ 45.48.010 et seq. | that possesses ***personal information***, including an individual's first or last name plus:<br>• SSN.<br>• Driver's license number or state identification card number.<br>• Account number, credit card number, or debit card number plus a personal code (e.g., PIN, password, etc.).<br>• Passwords, PINs, or other access codes for financial accounts. | personal information was subject to the breach "in the most expeditious time possible and without unreasonable delay" after discovering or being notified of the breach.<br><br>If the number of affected individuals exceeds 1,000, requires notice to consumer credit reporting agencies (unless the affected entity is subject to GLBA).<br><br>If a third-party (i.e., an "information recipient") experiences a breach, requires notification of the entity that owns or licenses the use of the personal information "as necessary" to ensure compliance. | notice exceeds $150,000, the affected class of Alaska residents exceeds 300,000, or the entity does not have sufficient contact information), permits notice via email, posting the disclosure on their website, and providing notice to major statewide media. | | ***Penalties***. Provides that a violation is an unfair or deceptive act or practice and subjects the entity to a civil penalty of up to $500 per state resident who was not notified, up to $50,000. |
| ***Arizona***<br><br>ARIZ. REV. STAT. §§ 18-551 et seq. | Applies to a business entity that conducts business in Arizona and that owns, maintains, or licenses unencrypted or un-redacted computerized ***personal information***, including an individual's first and last name plus:<br>• SSN.<br>• Driver's license number.<br>• Private key used to authenticate or sign an electronic record.<br>• Financial account number, debit card number, etc. | Requires notice via written document, email, or telephone to affected individuals within 45 days after the determination that a breach has occurred.<br><br>If the breach requires notification of more than 1,000 affected individuals, requires notice within 45 days of the breach to:<br>• The three largest nationwide consumer reporting agencies; and | In limited circumstances (i.e., the cost of providing notice exceeds $50,000, the affected class exceeds 100,000 individuals, or the entity does not have sufficient contact information), permits notice via a written letter to the attorney general demonstrating the need for substitute notice and a | Exempts or deems compliant certain entities from the breach notification requirements, including:<br>• Entities subject to federal requirements on data breach notification (i.e., GLBA, HIPAA).<br>• Entities with notification procedures that | ***Penalties***. Provides that a knowing and willful violation is an "unlawful practice" and allows the Attorney General to impose a civil penalty not to exceed $10,000 per affected individual or the total amount of economic loss |

| State | Covered Entities and Data | Method and Timing of Notice | Substitute Notice | Exceptions | Other |
|---|---|---|---|---|---|
| | plus any required security code or password that allows access to the account.<br>• Health insurance ID number.<br>• Information about a medical or mental health treatment or diagnosis by a health care professional.<br>• Passport number.<br>• TIN.<br>• Biometric data.<br><br>Includes an individual's user name/e-mail address plus a password (or security question and answer) that allows access to an online account, but does not include publicly available information. | • The Attorney General, in writing.<br><br>If a third-party (i.e., a person that maintains unencrypted and unredacted computerized personal information that the person does not own or license) experiences a breach, requires notification of the owner or licensee of the information "as soon as practicable" on discovering the breach. | conspicuous posting of the notice for at least 45 days on the entity's website. | are at least as thorough as these the timing requirements in the broad data breach notification law.<br><br>Deems sufficient for compliance notification requirements or security system breach procedures pursuant to requirements established by the primary or functional state or federal regulator. | sustained by affected individuals, up to $500,000. |
| ***Arkansas***<br><br>ARK. CODE ANN. §§ 4-110-101 et seq.; FAQs. | Applies to businesses that acquire, own, or license computerized data that includes Arkansas residents' ***personal information***, including an individual's first and last name plus:<br>• SSN.<br>• Driver's license number or other state ID number.<br>• Account number, credit card number, etc. plus any required security or access code. | Requires notice in writing or via email to affected individuals in the "most expedient time and manner possible without unreasonable delay."<br><br>If the breach requires notification of more than 1,000 affected individuals, requires notice to the three largest nationwide consumer reporting agencies and to the Attorney General. | In limited circumstances (i.e., the cost of providing notice exceeds $250,000, the affected class exceeds 500,000 Arkansas residents, or the entity does not have sufficient contact information), permits notice via email, conspicuous posting on the business' website, and | Exempts or deems compliant certain entities from the breach notification requirements, including:<br>• Entities with notification procedures that are at least as thorough as these the timing requirements in the broad data | ***Waivers***. Renders waivers contrary to public policy, void, and unenforceable.<br><br>***Penalties***. Provides that a violation is punishable by the Attorney General as an unfair trade practice. |

| State | Covered Entities and Data | Method and Timing of Notice | Substitute Notice | Exceptions | Other |
|---|---|---|---|---|---|
| | • Medical information.<br>• Biometric data. | If a third-party (i.e., a business that maintains computerized data that includes personal information that it does not own) experiences a breach, requires it to notify the owner or licensee that there has been a breach immediately following discovery. | notification by statewide media. | breach notification law. | |
| ***California***<br><br>CAL. CIVIL CODE § 1798.82; Recommended Practices on Notice of Security Breach Involving Personal Information. | Applies to businesses that conduct business in California and that own or license computerized data that includes ***personal information***, including an individual's first and last name plus:<br>• SSN.<br>• Driver's license number, California ID card number, TIN, passport number, etc.<br>• Account number or credit/debit card number plus any required security code, access code, or password.<br>• Medical information.<br>• Health insurance information.<br>• Biometric data.<br>• Information or data collected through the use or operation of an automated license plate recognition system. | Requires written or electronic notice to affected individuals "in the most expedient time possible and without unreasonable delay" following discovery or notification of the breach (i.e., per non-binding guidance from the California Office of Privacy Protection, recommends that notice be given within 10 business days of a determination that a breach occurred), as prescribed in the statute.<br><br>If the breach requires notification of more than 500 California residents, requires notice to the Attorney General.<br><br>If a third-party (i.e., a business that maintains computerized data that includes personal information that it does not own) experiences a breach, requires it to notify the owner or licensee that there has been a breach | In limited circumstances (i.e., the cost of providing notice exceeds $250,000, the affected class exceeds 500,000 California residents, or the entity does not have sufficient contact information), permits notice via email, conspicuous posting for at least 30 days on the business' website, and notification to major statewide media. | Exempts or deems compliant certain entities from the breach notification requirements, including:<br>• Entities subject to federal requirements on data breach notification (i.e., HIPAA, HITECH).<br>• Entities with notification procedures that are at least as thorough as these the timing requirements in the broad data breach notification law. | ***Private Right of Action***. Allows any injured customer to institute a civil action to recover damages.<br><br>***Waivers***. Renders waivers void/ unenforceable.<br><br>***Alternative Standards***. Provides a stringent data privacy framework under the California Consumer Privacy Act, Cal. Civil Code §§ 1798.100 et seq. |

| State | Covered Entities and Data | Method and Timing of Notice | Substitute Notice | Exceptions | Other |
|---|---|---|---|---|---|
| | • A username or email address plus a password or security question and answer that would permit access to an online account.<br><br>Does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. | immediately following discovery. | | | |
| ***Colorado***<br><br>COLO. REV. STAT. § 6-1-716 | Applies to businesses that—in the course of their business—maintain, own, or license ***personal information***, including a resident's first name and last name plus:<br>• SSN.<br>• Student, military, or passport identification number.<br>• Driver's license number or ID card number.<br>• Medical information.<br>• Health insurance identification number.<br>• Biometric data.<br>• A Colorado resident's username or email address plus a password or security question and answer. | Requires written, telephonic, or electronic notice to affected individuals within 30 days of the determination that a security breach occurred (i.e., unless the investigation into the breach determines that the misuse of information about a Colorado resident has not occurred/is not reasonably likely to occur).<br><br>If the breach requires notification of more than 500 Colorado residents, requires notice to the Attorney General within 30 days after the determination that a breach occurred.<br><br>If the breach requires notification of more than 1,000 | In limited circumstances (i.e., the cost of providing notice exceeds $250,000, the affected class exceeds 250,000 Colorado residents, or the entity does not have sufficient contact information), permits notice via email, conspicuous posting on the business' website, and notification to major statewide media. | Exempts or deems compliant certain entities from the breach notification requirements, including:<br>• Entities subject to federal requirements on data breach notification (i.e., GLBA).<br>• Entities with notification procedures that are at least as thorough as these the timing requirements in the broad data | ***Waivers***. Renders waivers void/ unenforceable.<br><br>***Penalties***. Permits the Attorney General to seek direct damages and injunctive relief. |

| State | Covered Entities and Data | Method and Timing of Notice | Substitute Notice | Exceptions | Other |
|---|---|---|---|---|---|
| | • A Colorado resident's account number or credit/debit card number plus any required security code, access code, of password.<br><br>Does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media. | Colorado residents, requires notice to all consumer reporting agencies "in the most expedient time possible and without unreasonable delay."<br><br>If a third-party service provider experiences a breach, requires it to notify the covered entity in the most expedient time possible and without unreasonable delay following discovery of a breach. | | breach notification law.<br><br>Deems sufficient for compliance notification requirements or security system breach procedures pursuant to requirements established by the primary or functional state or federal regulator. | |
| ***Connecticut***<br><br>CONN. GEN. STAT. § 36a-701b. | Applies to businesses that own, license, or maintain computerized data that includes ***personal information***, defined as an individual's first and last name plus:<br>• SSN, driver's license number, or state ID number.<br>• Credit or debit card number.<br>• Financial account number plus any required security code, access code, or password.<br><br>Does not include publicly available information that is lawfully made available to the general public from federal, state or local government | Requires written, telephonic, or electronic notice to affected individuals within 90 days of the discovery of the breach.<br><br>Requires notice to the Attorney General not later than the time when notice is provided to the residents.<br><br>If a third-party (i.e., a person that maintains computerized data that includes personal information that the person does not own) experiences a breach, requires it to notify the owner or licensee of the breach immediately following its discovery, if the personal information of a Connecticut resident was breached/reasonably believed to have been breached. | In limited circumstances (i.e., the cost of providing notice exceeds $250,000, the affected class exceeds 500,000 persons, or the entity does not have sufficient contact information), permits notice via email, conspicuous posting on the business' website, and notification to major statewide media. | Exempts or deems compliant certain entities from the breach notification requirements, including:<br>• Entities subject to federal requirements on data breach notification (i.e., HIPAA).<br>• Entities with notification procedures that are at least as thorough as these the timing requirements in the broad data breach notification law. | ***Insurance-Specific Standards***. Adopts the NAIC Data Security Model Law.<br><br>***Penalties***. Deems failure to comply with the notification requirements an unfair trade practice subject to enforcement by the Attorney General. |

| State | Covered Entities and Data | Method and Timing of Notice | Substitute Notice | Exceptions | Other |
|---|---|---|---|---|---|
| | records or widely distributed media. | | | Deems sufficient for compliance notification requirements or security system breach procedures pursuant to requirements established by the primary or functional state or federal regulator. | |
| ***Delaware***<br><br>DEL. CODE ANN. tit. 6 §§ 12B-101 et seq. | Applies to any person who conducts business in Delaware and that owns or licenses computerized data that includes ***personal information***, including a Delaware resident's first name or first initial and last name plus:<br>• SSN, TIN, driver's license number, or state ID number.<br>• Credit or debit card number plus any required security code, access code, or password.<br>• Passport number.<br>• Email address plus any required password or security question and answer.<br>• Medical history, medical treatment, diagnosis of | Requires written, telephonic, or electronic notice to affected individuals within 60 days of the determination of the breach.<br><br>If the breach requires notification of more than 500 Delaware residents, requires notice to the Attorney General within 60 days.<br><br>If a third-party (i.e., person that maintains computerized data that includes personal information that they do not own or license) experiences a breach, requires it to notify the owner or licensee of the breach immediately following determination of the breach. | In limited circumstances (i.e., the cost of providing notice exceeds $75,000, the affected class exceeds 100,000 residents, or the individual/entity does not have sufficient contact information), permits notice via email, conspicuous posting on the website of the entity, and notification to major statewide media. | Exempts or deems compliant certain entities from the breach notification requirements, including:<br>• Entities subject to federal requirements on data breach notification (i.e., GLBA, HIPAA).<br>• Entities with notification procedures that are at least as thorough as these the timing requirements in the broad data breach notification law. | ***Penalties***. Permits the Attorney General to bring an action to address violations and for other necessary relief to ensure compliance and recover damages. |

| State | Covered Entities and Data | Method and Timing of Notice | Substitute Notice | Exceptions | Other |
|---|---|---|---|---|---|
| | mental or physical condition, or DNA profile.<br>• Health insurance policy number, subscriber identification number, or etc.<br>• Biometric data.<br><br>Does not include publicly available information that is lawfully made available to the general public from federal, state or local government records. | | | Deems sufficient for compliance notification requirements or security system breach procedures pursuant to requirements established by the primary or functional state or federal regulator. | |
| ***District of Columbia***<br><br>D.C. CODE § 28-3851 et seq. | Applies to businesses that own or license computerized or other electronic data that includes ***personal information***, including an individual's first name/first initial and last name plus:<br>• SSN, TIN, passport number, driver's license number, unique identification number, etc.<br>• Account number, credit or debit card number plus any required security code, access code, or password.<br>• Medical information.<br>• Genetic information.<br>• Health insurance information (e.g., policy number, subscriber information number, etc.). | Requires prompt written or electronic notification of each District resident whose personal information was subject to the breach "in the most expeditious time possible and without unreasonable delay" after discovering the breach.<br><br>If the breach requires notification of more than 50 District residents, requires notice to the Attorney General "in the most expedient manner possible."<br><br>If the affected class exceeds more than 1,000 people, requires notice to all consumer reporting agencies, unless the business is already required to do so pursuant to GLBA. | In limited circumstances (i.e., the cost of providing notice exceeds $50,000, the affected class exceeds 100,000 people, or the entity does not have sufficient contact information), permits notice via email, conspicuous posting on the website of the entity, and notice to major local and (if applicable) national media. | Exempts or deems compliant certain entities from the breach notification requirements, including:<br>• Entities subject to federal requirements on data breach notification (i.e., GLBA, HIPAA, HITECH).<br>• Entities with notification procedures that are at least as thorough as these the timing requirements in the broad data | ***Penalties***. Provides that a violation is an unfair or deceptive trade practice and permits the Attorney General to seek direct damages and injunctive relief.<br><br>***Private Right of Action***. Allows any injured customer to institute a civil action to recover damages.<br><br>***Waivers***. Renders waivers void/ unenforceable. |

| State | Covered Entities and Data | Method and Timing of Notice | Substitute Notice | Exceptions | Other |
|---|---|---|---|---|---|
| | • Biometric data.<br>• Any combination of such data elements that would enable a person to commit identity theft without reference to a person's name.<br><br>Includes a user name/e-mail address plus a password (or security question and answer) that permits access to an email account. | If a third-party (i.e., an entity that maintains, handles, or otherwise possesses computerized or other electronic data that includes personal information that the person does not own) experiences a breach, requires it to notify the owner or licensee of the breach in the most expedient time possible following discovery. | | breach notification law. | |
| ***Florida***<br><br>FLA. STAT. § 501.171 | Applies to business entities that acquire, maintain, store, or use ***personal information***, including an individual's first name or first initial and last name plus:<br>• SSN, driver's license/ID card number, passport number, military identification number, etc.<br>• Financial account number, credit or debit card number plus any required security code, access code, or password.<br>• Medical information.<br>• Health insurance information.<br><br>Includes a user name/email address plus a password (or security question) and answer | Requires written or electronic notice to affected individuals within 30 days of the determination of the breach (or reason to believe a breach occurred).<br><br>If the breach requires notification of more than 500 Florida residents, requires notice to the Department of Legal Affairs within 30 days of the determination of the breach (or reason to believe a breach occurred).<br><br>If the breach requires notification of more than 1,000 individuals, requires notification of all consumer reporting agencies. | In limited circumstances (i.e., the cost of providing notice exceeds $250,000, the affected class exceeds 500,000 people, or the entity does not have an email or mailing address for the affected individuals), permits notice via conspicuous posting on the website of the entity and notice in print and to broadcast media. | Deems sufficient for compliance notification requirements or security system breach procedures pursuant to requirements established by the primary or functional state or federal regulator. | ***Penalties***. Treats violations of the notification requirements as unfair or deceptive trade practices and, in certain circumstances, entities may be liable for a civil penalty of at most $500,000.<br><br>***Private Right of Action***. Does not establish a private right of action. |

| State | Covered Entities and Data | Method and Timing of Notice | Substitute Notice | Exceptions | Other |
|---|---|---|---|---|---|
| | that would permit access to an online account.<br><br>Does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or encrypted/secured information. | If a third-party agent experiences a breach, requires it to notify the owner of the information within 10 days of the determination of the breach (or reason to believe the breach occurred). | | | |
| ***Georgia***<br><br>GA. CODE ANN. §§ 10-1-911 et seq. | Applies to "information brokers" or "data collectors" that maintain computerized data that includes ***personal information***, including an individual's first name or first initial and last name plus:<br>• SSN, driver's license number, or state ID number.<br>• Account number credit or debit card number (if circumstances exist where such a number could be used without additional identifying information).<br>• Account passwords, PINs, or other access codes.<br>• Any combination of such data elements that would enable a person to commit identity theft without reference to a person's name. | Requires written, telephonic, or electronic notice to affected residents "in the most expedient time possible and without unreasonable delay" following discovery or notification of the breach.<br><br>If the breach requires notification of more than 10,000 residents at one time, requires notice to all consumer reporting agencies "without unreasonable delay."<br><br>If a third-party (i.e., a person or business that maintains computerized data on behalf of an information broker or data collector but does not own it) experiences a breach, requires it to notify the information broker or data collector of the breach within 24 hours following discovery of the breach. | In limited circumstances (i.e., the cost of providing notice exceeds $50,000, the affected class exceeds 100,000 people, or the entity does not have sufficient contact information for the affected individuals), permits notice via email, conspicuous posting on the website of the entity, and notification to major statewide media. | Exempts or deems compliant certain entities from the breach notification requirements, including:<br>• Entities with notification procedures that are at least as thorough as these the timing requirements in the broad data breach notification law. | N/A |

| State | Covered Entities and Data | Method and Timing of Notice | Substitute Notice | Exceptions | Other |
|---|---|---|---|---|---|
| | Does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. | | | | |
| ***Hawaii***<br><br>HAW. REV. STAT. §§ 487N-1 et seq. | Applies to businesses that own or license ***personal information***, including an individual's first name or first initial and last name plus:<br>• SSN, driver's license number, or Hawaii ID card number.<br>• Account number, credit or debit card number, access code, or password that would permit access to an individual's financial accounts.<br><br>Does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. | Requires written, telephonic, or electronic notice to affected persons "without unreasonable delay" following discovery or notification of the breach.<br><br>If the breach requires notification of more than 1,000 persons, requires notice in writing "without unreasonable delay" of Hawaii's Office of Consumer Protection and all consumer reporting agencies.<br><br>If a third-party (i.e., a business that maintains or possesses records or data containing personal information of Hawaii residents that the business does not own or license) experiences a breach, requires it to notify the owner or licensee of the information immediately following discovery of the breach. | In limited circumstances (i.e., the cost of providing notice exceeds $100,000, the affected class exceeds 200,000 people, the entity does not have sufficient contact information or consent, or the business is unable to identify particular affected individuals), permits notice via email, conspicuous posting on the website of the entity, and notification to major statewide media. | Exempts or deems compliant certain entities from the breach notification requirements, including:<br>• Entities subject to federal requirements on data breach notification (i.e., HIPAA, Federal Interagency Guidance). | ***Penalties***. Subjects businesses that violate the notification rules to $2,500 penalties for each violation.<br><br>Authorizes the Attorney General or the Executive Director of the Office of Consumer Protection to bring an action.<br><br>***Private Right of Action***. Renders any business that violates the notification rules liable to the injured party in an amount equal to the sum of any actual damages sustained by the injured party. |

| State | Covered Entities and Data | Method and Timing of Notice | Substitute Notice | Exceptions | Other |
|---|---|---|---|---|---|
| | | | | | ***Waivers***. Renders waivers void/ unenforceable. |
| ***Idaho***<br><br>IDAHO CODE. § 28-51-104 et seq. | Applies to any commercial entity conducting businesses in Idaho that owns or licenses computerized data that includes ***personal information***, including the first name or first initial, and last name of an Idaho resident plus one of the following:<br>• SSN, driver's license number, Idaho ID number.<br>• Account number, credit or debit card number plus any required security code, access code, or password.<br><br>Does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. | Requires written, telephonic, or electronic notice to affected residents "in the most expedient time possible and without unreasonable delay" following discovery or notification of the breach.<br><br>If a third-party (i.e., a business that maintains or possesses records or data containing personal information of Idaho residents that the business does not own or license) experiences a breach, requires it to notify the owner or licensee of the information immediately following discovery of the breach. | In limited circumstances (i.e., the cost of providing notice exceeds $25,000, the affected class exceeds 50,000 people, or the entity does not have sufficient contact information), permits notice via email, conspicuous posting on the website of the entity, and notice to major statewide media. | Exempts or deems compliant certain entities from the breach notification requirements, including:<br>• Entities with notification procedures that are at least as thorough as these the timing requirements in the broad data breach notification law.<br><br>Deems sufficient for compliance notification requirements or security system breach procedures pursuant to requirements established by the primary or functional state or federal regulator. | ***Penalties***. Subjects businesses that intentionally violate the notification rules to a fine of no more than $25,000 per breach.<br><br>Authorizes the primary state regulator (e.g., the Department of Insurance or Attorney General) to bring a civil action. |
| ***Illinois*** | Applies to any "data collector" that, for any purpose, handles, collects, disseminates, or | Requires written or electronic notice to affected residents in "the most expedient time | In limited circumstances (i.e., the cost of providing | Exempts or deems compliant certain entities from the | ***Waivers***. Renders waivers void/ unenforceable. |

| State | Covered Entities and Data | Method and Timing of Notice | Substitute Notice | Exceptions | Other |
|---|---|---|---|---|---|
| 815 ILL. COMP. STAT. 530/5 | otherwise deals ***personal information***, including the first name or first initial, and last name of an Illinois resident plus:<br>• SSN.<br>• Driver's license number or Illinois ID card number.<br>• Account number, credit or debit card number, or in combination of such numbers, any required security code, access code, or password that would permit access to an individual's financial account.<br>• Medical information.<br>• Health insurance information (e.g., health insurance policy number, subscriber identification number, or any unique identifier, etc.).<br>• Biometric data.<br><br>Includes a user name/email address plus a password (or security question) and answer that would permit access to an online account.<br><br>Does not include publicly available information that is lawfully made available to the general public from federal, | possible and without unreasonable day" following discovery or notification of the breach.<br><br>Requires the notice include a statement with information for the individual to contact and obtain information from consumer reporting agencies and the Federal Trade Commission about fraud alerts and security freezes.<br><br>Prohibits the required notice from including information about the number of Illinois residents affected by the breach.<br><br>If the breach requires notification of more than 500 Illinois residents, requires notice to the Attorney General "in the most expedient time possible and without unreasonable delay" but no later than the consumer notice, including:<br>• A description of the nature of the breach.<br>• The number of Illinois residents affected at the time of notification.<br>• Any steps the data collector has taken or plans to take regarding the breach.<br><br>If a third-party (i.e., a business that maintains or possesses | notice exceeds $250,000, the affected class exceeds 500,000 people, or the entity does not have sufficient contact information), permits notice via email, conspicuous posting on the website of the entity, and notice to major statewide media or local media (if applicable). | breach notification requirements, including:<br>• Entities subject to federal requirements on data breach notification (i.e., HIPAA, HITECH).<br>• Entities with notification procedures that are at least as thorough as these the timing requirements in the broad data breach notification law. | ***Penalties***. Any violations constitute an unlawful practice under the Illinois Consumer Fraud and Deceptive Business Practices Act. |

| State | Covered Entities and Data | Method and Timing of Notice | Substitute Notice | Exceptions | Other |
|---|---|---|---|---|---|
| | state, or local government records. | records or data containing personal information of Illinois residents that the business does not own or license) experiences a breach, requires it to notify the owner or licensee immediately following discovery of the breach, including notice of the approximate date of the breach and the nature of the breach, and any steps the data collector has taken or plans to take regarding the breach. | | | |
| ***Indiana***<br><br>IND. CODE § 24-4.9-1 et seq.; Consumer Protection Division FAQ | Applies to any "data base owner" (e.g., a person or company that owns or licenses computerized data) that includes ***personal information***, including a SSN or an individual's first name or first initial, and last name plus any one or more of the following:<br>• Driver's license or ID card number.<br>• Credit card number.<br>• Account number or debit card number plus any required security or access code.<br><br>Does not include publicly available information that is lawfully made available to the general public from federal, | Requires written, electronic, or telephonic notice, "without unreasonable delay," to affected residents and Indiana's attorney general.<br><br>Requires notification to consumer reporting agencies if more than 1,000 Indiana residents are to be notified. | In limited circumstances (i.e., the cost of providing notice exceeds $250,000, the affected class exceeds 500,000 people), permits notice via conspicuous posting on the entity's website, and notification to geographically relevant statewide media. | Exempts or deems compliant certain entities from the breach notification requirements, including:<br>• Entities subject to federal requirements on data breach notification (i.e., GLBA, HIPAA, Patriot Act, Executive Order 13224, Driver Privacy Protection Act, Fair Credit Reporting Act).<br>• Entities with notification | ***Penalties***. Any violations constitute an unlawful practice under Indiana's deceptive practices law. |

| State | Covered Entities and Data | Method and Timing of Notice | Substitute Notice | Exceptions | Other |
|---|---|---|---|---|---|
| | state or local government records. | | | procedures that are at least as thorough as these the timing requirements in the broad data breach notification law. | |
| ***Iowa***<br><br>IOWA CODE § 715C.1 | Applies to any person (e.g., any legal or commercial entity, etc.) who owns or licenses computerized data that includes ***personal information***, including:<br>• SSN.<br>• Driver's license or unique government ID number.<br>• Account number, credit or debit card number plus any required security or access code.<br>• Biometric data.<br><br>Does <u>not</u> include publicly available information that is lawfully made available to the general public from federal, state or local government records. | Requires written or electronic notice to affected consumers "in the most expeditious manner possible and without unreasonable delay."<br><br>Requires notification to the Attorney General's Consumer Protection Division Director within five business days after notifying affected people. | In limited circumstances (i.e., the cost of providing notice exceeds $250,000, the affected class exceeds 350,000 people, or if there is not sufficient contact information), permits notice via conspicuous posting on the entity's website, and notification to geographically relevant statewide media. | Exempts or deems compliant certain entities from the breach notification requirements, including:<br>• Entities subject to federal requirements on data breach notification (i.e., GLBA, HIPAA).<br>• Entities with notification procedures that are at least as thorough as these the timing requirements in the broad data breach notification law.<br><br>Deems sufficient for compliance notification requirements or security system breach | ***Penalties***. Any violations constitute an unlawful practice under the Iowa Consumer Fraud Act. |

| State | Covered Entities and Data | Method and Timing of Notice | Substitute Notice | Exceptions | Other |
|---|---|---|---|---|---|
| | | | | procedures pursuant to requirements established by the primary or functional state or federal regulator. | |
| ***Kansas***<br><br>KAN. STAT. ANN. § 50–7a02 | Applies to any person (e.g., one that conducts business in Kansas, or a government, governmental subdivision or agency) that owns or licenses computerized data that includes ***personal information***, including.<br>• SSN.<br>• Driver's license number or Kansas ID card number.<br>• Financial account number, or credit or debit card number, alone or in combination with any required security code, access code or password<br><br>Does not include publicly available information that is lawfully made available to the general public from federal, state or local government records. | Requires a reasonable and good faith prompt investigation to determine the likelihood that personal information has been or will be misused. If the investigation determines that the misuse of information has occurred or is reasonably likely to occur, requires notice to affected Kansas residents.<br><br>In the event that there are more than 1,000 consumers to notify, requires notice, without unreasonable delay, to all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis. | In limited circumstances (i.e., the cost of providing notice exceeds $100,000, the affected class exceeds 5,000 people), permits notice via conspicuous posting on the entity's website, and notification to geographically relevant statewide media. | Exempts or deems compliant certain entities from the breach notification requirements, including:<br>• Entities with notification procedures that are at least as thorough as these the timing requirements in the broad data breach notification law.<br><br>Deems sufficient for compliance notification requirements or security system breach procedures pursuant to requirements established by the primary or functional state or federal regulator. | ***Penalties***. For violations, the attorney general is empowered to bring an action in law or equity (except against state licensed insurers). |
| | | | | | |

| State | Covered Entities and Data | Method and Timing of Notice | Substitute Notice | Exceptions | Other |
|---|---|---|---|---|---|
| ***Kentucky***<br><br>KY. REV. STAT. ANN. § 365.720 | Applies to any "information holder" (e.g., any person or business entity that conducts business in Kentucky) of ***personally identifiable information***, including an individual's first name or first initial and last name plus any one or more of the following:<br>• SSN.<br>• Driver's license number.<br>• Account number or credit or debit card number, plus any required security code or access code. | Requires written or electronic notice "in the most expedient time possible and without unreasonable delay" to any Kentucky resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.<br><br>In the event that there are more than 1,000 consumers to notify, requires notice, without unreasonable delay, to all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis. | In limited circumstances (i.e., the cost of providing notice exceeds $250,000, the affected class exceeds five hundred thousand 500,000, or the entity does not have sufficient contact information for the affected individuals), permits notice via email, conspicuous posting on the website of the entity, and notification to major statewide media. | Exempts or deems compliant certain entities from the breach notification requirements, including:<br>• Entities subject to federal requirements on data breach notification (i.e., GLBA, HIPAA).<br>• Entities with notification procedures that are at least as thorough as these the timing requirements in the broad data breach notification law. | ***Private Right of Action***. Allows any injured customer to institute a civil action to recover damages. |
| ***Louisiana***<br><br>LA. REV. STAT. § 51:3071 et seq | Applies to any person that conducts business in the state or that owns or licenses computerized data that includes ***personal information***, including the first name or first initial and last name of an individual resident of Louisiana plus any one or more of the following:<br>• SSN.<br>• Driver's license number or Louisiana ID card number. | Requires written or electronic notice "in the most expedient time possible and without unreasonable delay" but no later than 60 days from the discovery of the breach. | In limited circumstances (i.e., the cost of providing notice exceeds $100,000 or that the affected class of persons to be notified 100,000, or the person does not have sufficient contact information), permits notice via email, conspicuous posting on the business' | Exempts or deems compliant certain entities from the breach notification requirements, including:<br>• Entities subject to federal requirements on data breach notification (i.e., Federal Interagency Guidance). | ***Private Right of Action***. Allows any injured customer to institute a civil action to recover damages. |

| State | Covered Entities and Data | Method and Timing of Notice | Substitute Notice | Exceptions | Other |
|---|---|---|---|---|---|
| | • Account number, credit or debit card number, plus any required security code, access code, or password that would permit access to an individual's financial account.<br>• Passport number.<br>• Biometric data.<br><br>Does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. | | website, and notification to major statewide media. | | |
| ***Maine***<br><br>10 ME. REV. STAT. § 1346 et seq. | Applies to "information brokers" that maintain computerized data that includes ***personal information***, including an individual's first name, or first initial, and last name in combination with any one or more of the following data elements:<br>• SSN;<br>• Driver's license number or Maine ID card number<br>• Account number, credit card number or debit card number.<br>• Account passwords or personal identification numbers or other access codes. | Requires written or electronic notice "as expediently as possible and without unreasonable delay" to affected residents.<br><br>If the breach requires notice of more than 1,000 individuals, requires notice of all consumer reporting agencies.<br><br>If a third-party (i.e., a person or business that maintains computerized data on behalf of an information broker or data collector but does not own it) experiences a breach, requires notice to the information broker or data collector of the breach. | In limited circumstances (i.e., the cost of providing notice exceeds $5,000, that the affected class exceeds 1,000, or the entity does not have sufficient contact information), permits notice via email, conspicuous posting on the business' website, and notification to major statewide media. | N/A | ***Penalties***. Provides that a person that violates the notice requirements is subject to one or more of the following:<br>• A fine of no more than $500 per violation, up to $2,500 per day;<br>• Equitable relief; or<br>• Enjoinment from further violations. |

| State | Covered Entities and Data | Method and Timing of Notice | Substitute Notice | Exceptions | Other |
|---|---|---|---|---|---|
| | | Requires notice to the appropriate state regulators within the Department of Professional and Financial Regulation, or if the person is not regulated by the department, Maine's Attorney General. | | | |
| ***Maryland***<br><br>MD. CODE COM. LAW § 14-3501 et seq. | Applies to any business that owns, licenses, or maintains computerized data that includes ***personal information***, including an individual's first name or first initial and last name plus any one or more of the following:<br>• SSN, ITIN, passport number, or other ID number issued by the federal government.<br>• Driver's license number or Maryland ID card number.<br>• Account number, credit card number, or debit card number, plus any required security code, access code, or password.<br>• Medical information, including information about an individual's mental health.<br>• Health insurance information (e.g., health insurance policy number, certificate number, or health insurance subscriber | Requires written, telephonic, or electronic notice to affected residents notice as soon as reasonably practicable, but no later than 45 days after discovery or notification of a breach of the security of a system.<br><br>If the breach requires notification of more than 1,000 individuals, requires notification of all consumer reporting agencies. | In limited circumstances (i.e., the cost of providing notice exceeds $100,000, that the affected class exceeds 175,000, or the entity does not have sufficient contact information), permits notice via email, conspicuous posting on the business' website, and notification to statewide media. | Exempts or deems compliant certain entities from the breach notification requirements, including:<br>• Entities subject to federal requirements on data breach notification (i.e., GLBA, HIPAA).<br><br>Deems sufficient for compliance notification requirements or security system breach procedures pursuant to requirements established by the primary or functional state or federal regulator. | ***Waivers***. Renders waivers void/ unenforceable. |

| State | Covered Entities and Data | Method and Timing of Notice | Substitute Notice | Exceptions | Other |
|---|---|---|---|---|---|
| | ID number, plus a unique identifier).<br>• Biometric data.<br>• A user name or e-mail address plus a password or security question and answer that permits access to an individual's e-mail account. | | | | |
| ***Massachusetts***<br><br>MASS. GEN. LAWS 93H § 1 et seq. | Applies to any person, corporation, association, partnership or other legal entity that maintains or stores data that includes ***personal information***, including a resident's first name and last name or first initial and last name plus any one or more of the following:<br>• SSN.<br>• Driver's license number or state ID number.<br>• Account number, or credit or debit card number, with or without any required security or access code.<br><br>Does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. | Requires written or electronic notice "as soon as practicable and without unreasonable delay," to the attorney general, the director of consumer affairs and business regulation and affected residents. | In limited circumstances (i.e., the cost of providing written notice exceeds $250,000, or that the affected class exceeds 500,000 Massachusetts residents, or the entity does not have sufficient contact information to provide notice), permits notice via email, conspicuous posting on the business' website, and notification by statewide media. | Deems sufficient for compliance notification requirements or security system breach procedures pursuant to requirements established by the primary or functional state or federal regulator. | ***Private Right of Action***. Prohibits an entity from requiring a resident to waive the resident's right to a private right of action as a condition of offering credit monitoring services.<br><br>***Credit Monitoring Services***. If a breach includes a SSN, requires the entity to contract with a third party to offer each resident free credit monitoring services for at least 18 months (unless the entity is a consumer |

| State | Covered Entities and Data | Method and Timing of Notice | Substitute Notice | Exceptions | Other |
|---|---|---|---|---|---|
| | | | | | reporting agency—which, in that case, must contract with a third party to offer free credit monitoring services for at least 42 months. |
| ***Michigan***<br><br>MICH. COMP. LAWS § 445.63, 72 et seq. | Applies to any person that maintains ***personal information***, including a resident's first name or first initial and last name plus any one or more of the following:<br>• SSN.<br>• Driver's license number or Michigan ID number.<br>• Account number, credit card, or debit card number plus any required security or access code. | Requires written or electronic notice "without unreasonable delay" to affected residents.<br><br>If the breach requires notification of more than 1,000 residents at one time, requires notice to all consumer reporting agencies "without unreasonable delay." | In limited circumstances (i.e., the cost of providing notice exceeds $250,000, that the affected class exceeds 500,000), permits notice via email, conspicuous posting on the business' website, and notification to statewide media. | Exempts or deems compliant certain entities from the breach notification requirements, including:<br>• Entities subject to federal requirements on data breach notification (i.e., HIPAA, Federal Interagency Guidance, insurers). | ***Penalties***. Subjects a person that knowingly fails to provide any notice of a security breach to a civil fine of no more than $250.00 for each failure to provide notice (no more than $750,000 in aggregate). |
| ***Minnesota***<br><br>MINN. STAT. § 325E.61, 325E.64 | Applies to any person or business that owns or licenses data that includes ***personal information,*** including:<br>• SSN.<br>• Driver's license number or ID card number.<br>• Account number, credit card, or debit card number | Requires written or electronic notice immediately following discovery of a security breach.<br><br>If the breach requires notification of more than 500 residents at one time, requires notice to all consumer reporting agencies within 48 hours. | In limited circumstances (i.e., the cost of providing notice exceeds $250,000, that the affected class exceeds 500,000, or the entity does not have sufficient contact information), permits | Exempts or deems compliant certain entities from the breach notification requirements, including:<br>• Entities subject to federal requirements on data breach | ***Waivers***. Renders waivers void/ unenforceable. |

| State | Covered Entities and Data | Method and Timing of Notice | Substitute Notice | Exceptions | Other |
|---|---|---|---|---|---|
| | plus any required security or access code.<br><br>Does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. | | notice via email, conspicuous posting on the business' website, and notification to statewide media. | notification (i.e., HIPAA). | |
| ***Mississippi***<br><br>MISS. CODE § 75-24-29 | Applies to any person that conducts business that owns, licenses, or maintains ***personal information***, including an individual's first name or first initial and last name in combination with any one or more of the following data elements:<br>• SSN<br>• Driver's license number or state identification card number.<br>• Financial account number or credit or debit card plus any required security code, access code or password.<br><br>Does not include publicly available information lawfully available to the general public from government records or widely distributed media. | Requires notice via written, telephonic, or electronic methods. | In limited circumstances (i.e., there are more than 5,000 affected individuals), permits notice via electronic mail, conspicuous posting of the notice on the web site of the person if the person maintains one, and notification to major statewide media. | Exempts or deems compliant certain entities from the breach notification requirements, including:<br>• Entities with notification procedures that are at least as thorough as these the timing requirements in the broad data breach notification law.<br><br>Deems sufficient for compliance notification requirements or security system breach procedures pursuant to requirements established by the primary or functional | ***Penalties***. Provides that failure to comply shall constitute an unfair trade practice.<br><br>***Private Right of Action.*** Provides that a violation does not establish a private cause of action. |

| State | Covered Entities and Data | Method and Timing of Notice | Substitute Notice | Exceptions | Other |
|---|---|---|---|---|---|
| | | | | state or federal regulator. | |
| ***Missouri***<br><br>MO. REV. STAT. § 407.1500 | Applies to any business or person that conducts business in the state that owns or licenses ***personal information***, including an individual's first name or first initial and last name plus:<br>• SSN<br>• Driver's license number or other unique identification number.<br>• Financial account number, credit card number, or debit card number plus any required security code, access code, or password.<br>• Unique electronic identifier or routing code, plus any required security code, access code, or password.<br>• Medical information.<br>• Health insurance information.<br><br>Does not include publicly available information lawfully available to the general public. | Requires written, electronic, or telephonic notice that includes a description of the incident in general terms, the type of personal information that was obtained as a result of the breach of security, telephone number that the affected consumer may call for further information and assistance, if one exists, contact information for consumer reporting agencies, and advice that directs the affected consumer to remain vigilant by reviewing account statements and monitoring free credit reports.<br><br>If the breach requires notification of more than 1,000 affected individuals, requires notice to:<br>• The Attorney General<br>• Consumer reporting agencies in accordance with federal law | In limited circumstances (i.e., if the cost of providing notice would exceed $100,000, or if there are more than 150,000 affected individuals), permits notice via email, conspicuous posting of the notice or a link to the notice on the website of the person, and notification to major statewide media. | Exempts or deems compliant certain entities from the breach notification requirements, including:<br>• Entities subject to federal requirements on data breach notification (i.e., Federal Interagency Guidance).<br>• Entities subject to state requirements on data breach notification that are at least as thorough as these the requirements in the broad data breach notification law. | ***Penalties.*** Provides that the attorney general has exclusive authority to bring an action to obtain actual damages for a willful and knowing violation and may seek a civil penalty not to exceed $150,000 per preach of the security of the system or series of breaches of a similar nature that are discovered in a single investigation. |
| ***Montana***<br><br>MONT. CODE § 2-6-1501 et seq, 30-14- | Applies to any person or business that conducts business in the state or licenses data that includes ***personal information***, | Requires notice via written or telephonic means. Electronic notice is permitted if the notice provided is consistent with | In limited circumstances (i.e., if the cost of providing notice would exceed | Exempts or deems compliant certain entities from the breach notification | N/A |

| State | Covered Entities and Data | Method and Timing of Notice | Substitute Notice | Exceptions | Other |
|---|---|---|---|---|---|
| 1704 et seq., 33-19-321 | including an individual's first name or first initial and last name plus:<br>• SSN<br>• Driver's license number, state identification card number, or tribal identification card number.<br>• Account number or credit or debit card number plus required security code, access code, or password<br>• Medical record information.<br>• A TIN.<br>• An identity protection personal identification number issued by the United States Internal Revenue Service.<br><br>Does not include information that has lawfully been made available to the general public or that is encrypted. | federal law regarding electronic records and signatures.<br><br>Requires electronic notification to the Attorney General and Insurance Commissioner. | $250,000, if there are over 500,000 affected individuals, or if the person or business does not have sufficient contact information), permits notice via email and either conspicuous posting of the notice on the entity's website or notification to applicable local or statewide media. | requirements, including:<br>• Entities that maintain notification procedures that do not unreasonably delay notice and are at least as thorough as these the requirements in the broad data breach notification law. | |
| ***Nebraska***<br><br>NEB. REV. STAT. § 87-801 et seq. | Applies to any individual or person that conducts business in the state and that owns or licenses computerized data that includes ***personal information*** which is defined as:<br>• SSN<br>• Driver's license number or state identification card number. | Requires notice via written or telephonic method or electronic notice if consistent with federal law.<br><br>If a third party (i.e., an "entity that maintains computerized data") experiences a breach, requires notice to and | In limited circumstances (i.e., if the cost of providing notice will exceed $10,000), permits notice via email, notification by a paid advertisement in a local newspaper, conspicuous posting of | Exempts or deems compliant certain entities from the breach notification requirements, including:<br>• Entities that maintain notification procedures that | ***Penalties.*** Provides that the Attorney General may issue subpoenas and seek and recover direct economic damages for each resident injured. |

| State | Covered Entities and Data | Method and Timing of Notice | Substitute Notice | Exceptions | Other |
|---|---|---|---|---|---|
| | • Account or credit card or debit card number plus required security code, access code, or password.<br>• Unique electronic ID number or routing code plus required security code, access code, or password.<br>• Biometric data.<br>• User name or email address plus password or security question and answer.<br><br>Does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. | cooperation with the owner or licensee of the information. | the notice on the entity's web site, and notification to major media outlets in the geographic area in which the entity is located. | do not unreasonably delay notice and are at least as thorough as these the requirements in the broad data breach notification law.<br><br>Deems sufficient for compliance notification requirements or security system breach procedures pursuant to requirements established by the primary or functional state or federal regulator. | ***Waivers***. Provides that waivers are not permitted. |
| ***Nevada***<br><br>NEV. REV. STAT. § 603A.010 et seq., 242.183 | Applies to any entity that owns or licenses computerized data that includes ***personal information***, defined as a natural person's first name or first initial and last name plus:<br>• SSN<br>• Driver's license number, driver authorization card number or identification card number.<br>• Account number, credit card number or debit card number plus required | Requires written or electronic notice if consistent with federal law.<br><br>If a third-party (i.e., an entity that maintains computerized data that includes personal information that the entity does not own) experiences a breach, requires it to notify the owner or licensee of the breach immediately following discovery. | In limited circumstances (i.e., the cost of providing notification would exceed $250,000, the affected class of subject persons to be notified exceeds 500,000 or the data collector does not have sufficient contact information), permits notice via electronic mail, conspicuous posting of the | Exempts or deems compliant certain entities from the breach notification requirements, including:<br>• Entities subject to federal requirements on data breach notification (i.e., GLBA).<br>• Entities subject to state requirements on data breach | ***Penalties.*** Provides that the Attorney General may bring an action against violators to obtain a temporary or permanent injunction against the violation.<br><br>***Private Right of Action.*** Allows data collectors to commence an |

| State | Covered Entities and Data | Method and Timing of Notice | Substitute Notice | Exceptions | Other |
|---|---|---|---|---|---|
| | security code or access code.<br>• A medical identification number or a health insurance identification number.<br>• A user name, unique identifier or electronic mail address in combination with a password, access code or security question and answer that would permit access to an online account.<br><br>Does not include the last four digits of SSN, last four digits of a driver authorization card number, last four digits of an identification card number, or publicly available information that is lawfully made available to the general public from federal, state, or local government records. | | notification on the website of the data collector, and notification to major statewide media. | notification that are at least as thorough as these the requirements in the broad data breach notification law. | action for damages against a person that unlawfully obtained or benefitted from personal information obtained from records maintained by the data collector. |
| ***New Hampshire***<br><br>N.H. REV. STAT. § 359-C:19 et seq. | Applies to any individual or entity doing business in the state that owns or licenses computerized data that includes ***personal information***, defined as an individual's first name or initial and last name plus:<br>• SSN<br>• Driver's license number or other government identification number. | Requires notice via written, telephonic, or electronic means. Also permits notice pursuant to internal notification procedures maintained as part of an information security policy.<br><br>If a third-party (i.e., an entity that maintains computerized data that includes personal information that the entity does | In limited circumstances (i.e., the cost of providing notice would exceed $5,000, the affected class of subject individuals to be notified exceeds 1,000), permits notice via email, conspicuous posting of the notice | Deems sufficient for compliance notification requirements or security system breach procedures pursuant to requirements established by the primary or functional state or federal regulator. | ***Private Right of Action.*** Provides that any person injured by any violation may bring a civil action and recover actual damages and fees. If the act was willful or knowing, permits |

| State | Covered Entities and Data | Method and Timing of Notice | Substitute Notice | Exceptions | Other |
|---|---|---|---|---|---|
| | • Account number, credit card number, or debit card number, in combination plus security code, access code, or password.<br><br>Does not include information lawfully made available to the general public from federal, state, or local government records. | not own) experiences a breach, requires it to notify and cooperate with the owner or licensee of the breach immediately following discovery. | on the entity's website, and notification to major statewide media. | | up to three times but not less than two times such amount.<br><br>***Waivers.*** Does not permit waivers. |
| ***New Jersey***<br><br>N.J. STAT. § 56:8-163 | Applies to any entity conducting business in the state that complies or maintains computerized records that include ***personal information***, defined as an individual's first name or first initial and last name linked with any one or more of the following data elements:<br>• SSN<br>• Driver's license number or state identification card number.<br>• Account number or credit or debit card number plus any required security code, access code, or password.<br>• User name, email address, or any other account holder identifying information, plus any password or security question | Requires notice via written, telephonic means. Permits electronic notice for breaches involving online account credentials only except for email account credentials.<br><br>If a third-party (i.e., an entity that maintains computerized data that includes personal information that the entity does not own) experiences a breach, requires it to notify and cooperate with the owner or licensee of the breach immediately following discovery.<br><br>Requires notification to the Division of State Police in the Department of Law and Public Safety prior to customer disclosure. | In limited circumstances (i.e., the cost of providing notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000), permits notice via email, conspicuous posting of the notice on the entity's web site, and notification to major statewide media. | Exempts or deems compliant certain entities from the breach notification requirements, including:<br>• Entities subject to state requirements on data breach notification that are at least as thorough as these the requirements in the broad data breach notification law. | N/A |

| State | Covered Entities and Data | Method and Timing of Notice | Substitute Notice | Exceptions | Other |
|---|---|---|---|---|---|
| | • Dissociated data that, if linked, would constitute personal information.<br><br>Does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media. | Requires notification to consumer reporting agency if breach involves more than 1,000 persons at one time. | | | |
| ***New Mexico***<br><br>N.M. STAT. 57-12C-1 et seq. | Applies to any person that owns or licenses elements that include ***personal identifying information***, defined as an individual's first name or first initial and last plus:<br>• SSN<br>• Driver's license number.<br>• Government-issued identification number.<br>• Account number, credit card number or debit card plus any required security code, access code or password<br>• Biometric data.<br><br>Does not include publicly available information that is lawfully made available to the general public. | Requires notice "in the most expedient time possible" but not later than 45 days following discovery via United States mail. Permits electronic notification if the person required to make the notification primarily communicates with the New Mexico resident by electronic means.<br><br>Requires notification to the Attorney General and consumer reporting agencies if more than 1,000 residents are affected. | In limited circumstances (i.e., the cost of providing notification would exceed one hundred thousand dollars ($100,000), the number of residents to be notified exceeds fifty thousand), permits notice via electronic email, conspicuous posting on the business' website, and written notification to the office of the Attorney General and major media outlets in the state. | Exempts or deems compliant certain entities from the breach notification requirements, including:<br>• Entities subject to federal requirements on data breach notification (i.e., HIPAA, GLBA).<br>• Entities subject to state requirements on data breach notification that are at least as thorough as these the requirements in the broad data breach notification law. | ***Penalties.*** Provides that the Attorney General may bring an action against violators for an injunction and damages. Civil penalties of the greater of $25,000 or $10 per instance of failed notification up to a maximum of $150,000. |
| ***New York*** | | | | | |

| State | Covered Entities and Data | Method and Timing of Notice | Substitute Notice | Exceptions | Other |
|---|---|---|---|---|---|
| N.Y. GEN. BUS. LAW § 899-aa | Applies to any person, business, or state entity which conducts business in the state and which owns or licenses computerized data which includes ***private information*** defined any information plus:<br>• SSN<br>• Driver's license number or non-driver identification card number.<br>• Account number, credit or debit card number plus any required security code, access code, password or other information that would permit access to an individual's financial account.<br>• Account number, credit or debit card number, if such number could be used to access an individual's financial account without additional identifying information, security code, access code, or password.<br>• Biometric data.<br>• User name or e-mail address plus password or security question and answer.<br><br>Does not include publicly available information that is lawfully made available to the general public. | Requires written notice. Telephonic notice is permitted provided that the entity maintains a log of each notification. Electronic notice is permitted provided there is consent of the recipient and a log is maintained.<br><br>If a third-party (i.e., an entity that maintains computerized data that includes personal information that the entity does not own) experiences a breach, requires it to notify and cooperate with the owner or licensee of the breach immediately following discovery.<br><br>Requires notice to the Attorney General and the state consumer protection board if any state residents are to be notified. | In limited circumstances (i.e., providing notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000) permits notice via email, conspicuous posting on the entity's website, and notification to major statewide media. | Exempts or deems compliant certain entities from the breach notification requirements, including:<br>• Entities subject to federal requirements on data breach notification (i.e., GLBA, HIPAA).<br>• Entities subject to other state requirements regarding data breach notification (i.e., Part 500 of Title 23 of the New York State Code, other data security rules and regulations administered by official departments of the New York). | ***Penalties.*** Provides that the Attorney General may bring an action to restrain the continuation of violation. |

| State | Covered Entities and Data | Method and Timing of Notice | Substitute Notice | Exceptions | Other |
|---|---|---|---|---|---|
| | | | | | |
| ***North Carolina***<br><br>N.C. GEN. STAT. §§ 75-61, 75-65 | Applies to any organization that owns or licenses ***personal information*** defined as a person's first name or first initial and last name plus:<br>• SSN or employer TINs.<br>• Driver's license, State identification card, or passport number.<br>• Checking account numbers.<br>• Savings account numbers.<br>• Credit card numbers.<br>• Debit card numbers.<br>• Personal Identification (PIN) Code.<br>• Electronic identification numbers, electronic mail names or addresses.<br>• Internet account numbers, or Internet identification names.<br>• Digital signatures.<br>• Any other numbers or information that can be used to access a person's financial resources.<br>• Biometric data.<br>• Fingerprints.<br><br>In certain circumstances (i.e. the information would permit access to a financial account), may also include:<br>• Electronic ID numbers. | Requires written, telephonic, or electronic notice without unreasonable delay. Requires notice to be "clear and conspicuous" and include all of the following:<br>• A description of the incident in general terms.<br>• The type of personal information that was subject to the unauthorized access and acquisition.<br>• The general acts of the business to protect the personal information from further unauthorized access.<br>• A telephone number for the business that the person may call for further information<br>• Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports.<br>• The toll-free numbers and addresses for the major consumer reporting agencies.<br>• The toll-free numbers, addresses, and Web site addresses for the Federal Trade Commission and the North Carolina Attorney General's Office, along with a statement that the | In limited circumstances (i.e., if the cost of providing notice would exceed $250,000 or that the affected class of subject persons to be notified exceeds 500,000), permits notice via email, conspicuous posting of the notice on the entity's web site and notification to major statewide media. | Exempts or deems compliant certain entities from the breach notification requirements, including:<br>• Entities subject to federal requirements on data breach notification (i.e., Federal Interagency Guidance). | ***Waivers.*** Renders waivers void/ unenforceable.<br><br>***Private Right of Action.*** Provides that no private right of action may be brought by an individual unless the individual is injured as a result of the violation.<br><br>***Penalties.*** Provides that the Attorney General may enforce via civil and criminal penalties. |

| State | Covered Entities and Data | Method and Timing of Notice | Substitute Notice | Exceptions | Other |
|---|---|---|---|---|---|
| | • Email names or addresses.<br>• Internet account numbers.<br>• Internet ID names.<br>• Passwords.<br>• Parent's legal surname prior to marriage. | individual can obtain information from these sources about preventing identity theft.<br><br>If the breach requires notification of more than 1,000 people, requires notice to consumer reporting agencies.<br><br>If a third-party (i.e., a "third party agent") experiences a breach, requires notification immediately following discovery of the breach. | | | |
| ***North Dakota***<br><br>N.D. CENT. CODE § 51-30-01 et seq. | Applies to any entity that conducts business in the state that owns or licenses computerized data that includes ***personal information***, defined as an individual's first name or first initial and last name plus:<br>• SSN<br>• Driver's license number.<br>• A nondriver color photo identification card number assigned by the Department of Transportation.<br>• Account number, credit card number, or debit card number plus any required security code, access code, or password. | Requires notice via written or electronic methods.<br><br>If the breach requires notification of more than 250 people, requires notice to the Attorney General by mail or email.<br><br>If a third-party (i.e., a "third party agent") experiences a breach, requires notification immediately following discovery of the breach. | In limited circumstances (i.e., if the cost of providing notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000), permits notice via email, conspicuous posting of the notice on the entity's web site and notification to major statewide media. | Exempts or deems compliant certain entities from the breach notification requirements, including:<br>• Entities subject to federal requirements on data breach notification (i.e., Federal Interagency Guidance, entities subject to Title 45 of the Code of Federal Regulations). | N/A |

| State | Covered Entities and Data | Method and Timing of Notice | Substitute Notice | Exceptions | Other |
|---|---|---|---|---|---|
| | • Date of birth.<br>• Mother's maiden name.<br>• Medical information.<br>• Health insurance information.<br>• An identification number assigned to the individual by the individual's employer plus any required security code, access code, or password.<br>• Digital or other electronic signature.<br><br>Does not include information that has lawfully been made public or that is truncated, encrypted, secured, deidentified, etc. | | | | |
| ***Ohio***<br><br>OHIO REV. CODE § 1347.12, 1349.19, 1349.191, 1349.192 | Applies to any individual or entity that conducts business in the state and owns or licenses computerized data that includes ***personal information***, defined as an individual's first name or first initial and last name, plus:<br>• SSN<br>• Driver's license number or state identification card number.<br>• Account number or credit or debit card number plus any required security code, access code, or password. | Requires notice "in the most expedient time possible" following discovery via written, electronic, or telephonic means.<br><br>If a third-party (i.e., a "third party agent") experiences a breach, requires notification "in an expeditious manner" following discovery of the breach.<br><br>If the breach requires notification of more than 1,000 residents, requires notice to | In limited circumstances (i.e., if the cost of providing notice exceeds $250,000), permits notice via electronic mail, conspicuous posting on the entity's website, and notification to major media outlets that equal or exceed 75% of the population of the state. | Exempts or deems compliant certain entities from the breach notification requirements, including:<br>• Entities subject to federal requirements on data breach notification.<br>• Entities with preexisting contracts if it does not conflict | ***Penalties.*** Provides that the Attorney General may enforce via civil action. |

| State | Covered Entities and Data | Method and Timing of Notice | Substitute Notice | Exceptions | Other |
|---|---|---|---|---|---|
| | Does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. Also does not include widely distributed news, reporting, or nonprofit publication. | consumer reporting agencies and compilation and maintenance of files on consumers on a nationwide basis of the timing, distribution, and content of the disclosure given by the Entity to the residents. | | with any provisions of the broad notification requirement.<br><br>The consumer reporting agency requirement does not apply to certain entities with healthcare data in accordance with federal law. | |
| ***Oklahoma***<br><br>24 OKLA. STAT. § 161 et seq. | Applies to any entity that owns or licenses computerized data that includes ***personal information***, defined as the first name or first initial and last plus:<br>• SSN<br>• Driver license number or state identification card number issued in lieu of a driver license.<br>• Financial account number, or credit card or debit card number, plus any required security code, access code, or password.<br><br>Does not include information lawfully obtained from publicly available information or from federal, state, or local government records lawfully | Requires written, telephonic, or electronic notice "without unreasonable delay" following discovery or notification.<br><br>If a third-party (i.e., a "third party agent") experiences a breach, requires notification as soon as practicable but not later than 10 days after discovery. | In limited circumstances (i.e., if the cost of providing notice will exceed $50,000 or the affected class of residents to be notified exceeds 100,000 persons, permits notice via any two of the following: email notice, conspicuous posting of the notice on the entity's website, and notice to major statewide media. | Exempts or deems compliant certain entities from the breach notification requirements, including:<br>• Entities subject to federal requirements on data breach notification (i.e. Federal Interagency Guidance).<br>• Entities subject to state requirements on data breach notification that are at least as thorough as these the requirements in the broad data breach notification law. | ***Penalties.*** Provides that the Attorney General or district attorney has the authority to bring an action for actual damages or a civil penalty not to exceed $150,000 per breach or series of breaches of a similar nature that are discovered in a single investigation. |

| State | Covered Entities and Data | Method and Timing of Notice | Substitute Notice | Exceptions | Other |
|---|---|---|---|---|---|
| | made available to the general public. | | | Deems sufficient for compliance notification requirements or security system breach procedures pursuant to requirements established by the primary or functional state or federal regulator. | |
| ***Oregon***<br><br>OR. REV. STAT. §§ 646A.600, 646A.602, 646A.604, 646A.624, 646A.626 | Applies to any individual or entity that owns, licenses, maintains, stores, manages, collects, processes, acquires, or possesses ***personal information*** defined as a consumer's first name or first initial and last name plus:<br>• SSN<br>• Driver license number or state identification card number issued by the Department of Transportation.<br>• Passport number or other identification number.<br>• Financial account number, credit card number or debit card number plus any required security code, access code or password. | Requires notice in the "as soon as is practicable" and "without unreasonable delay" not to exceed 45 days after discovering or having reason to believe a breach of security has occurred via written, electronic, or telephonic means.<br><br>Requires Attorney General notification if the breach involved more than 250 or an undeterminable number of consumers.<br><br>If a third-party (i.e., a "third party agent") experiences a breach, requires notification as soon as practicable but not later than 10 days after discovery. | In limited circumstances (i.e., if the cost of notification would exceed $250,000 or the affected class of consumers exceeds 350,000) via conspicuous posting on the entity's website and notification to major statewide media. | Exempts or deems compliant certain entities from the breach notification requirements, including:<br>• Entities subject to federal requirements on data breach notification (i.e., GLBA, HIPAA, HITECH, other more restrictive requirements).<br><br>Deems sufficient for compliance notification requirements or security system breach procedures pursuant to requirements established by the | ***Penalties.*** Provides that violation of the statute is an unlawful trade practice. |

| State | Covered Entities and Data | Method and Timing of Notice | Substitute Notice | Exceptions | Other |
|---|---|---|---|---|---|
| | • Data from automatic measurements of a consumer's physical characteristics (e.g. fingerprint, retina or iris) used to authenticate identity in a transaction.<br>• Health insurance policy number or health insurance subscriber identification number plus any other unique identifier.<br>• Any information about a consumer's medical history or mental or physical condition or about a health care professional's medical diagnosis or treatment of the consumer.<br>• A user name or other means of identifying a consumer for the purpose of permitting access to the consumer's account plus any other method necessary to authenticate the user name or means of identification.<br><br>Does not include publicly available information that is lawfully made available to the | | | primary or functional state or federal regulator.<br><br>In these limited circumstances, requires notification to the state Attorney General. | |

| State | Covered Entities and Data | Method and Timing of Notice | Substitute Notice | Exceptions | Other |
|---|---|---|---|---|---|
| | general public from federal, state, or local government records. | | | | |
| ***Pennsylvania***<br><br>73 PA. STAT. § 2301 et seq. | Applies to any entity that maintains, stores, or manages computerized data that includes ***personal information*** which is defined as an individual's first name or first initial and last name plus:<br>• SSN<br>• Driver's license number or a State identification card number issued in lieu of a driver's license.<br>• Financial account number, credit or debit card number plus any required security code, access code or password that would permit access to an individual's financial account.<br><br>Does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. | Requires notice "without unreasonable delay" via written, telephonic, or electronic methods.<br><br>Requires notice to national consumer reporting agencies if notification to more than 1,000 persons is required. | In limited circumstances (i.e., the cost of providing notice would exceed $100,000 or the affected class of subject persons to be notified exceeds 175,000), permits notice via electronic mail, conspicuous posting on the entity's website, and notification to major statewide media. | Exempts or deems compliant certain entities from the breach notification requirements, including:<br>• Entities subject to federal requirements on data breach notification (i.e. Federal Interagency Guidance).<br>• Entities that maintain their own notification procedures that are at least as thorough as these the requirements in the broad data breach notification law.<br><br>Deems sufficient for compliance notification requirements or security system breach procedures pursuant to requirements established by the | ***Penalties.*** Provides that the Attorney General may bring an action for violations as an unfair trade practice. |

| State | Covered Entities and Data | Method and Timing of Notice | Substitute Notice | Exceptions | Other |
|---|---|---|---|---|---|
| | | | | primary or functional state or federal regulator. | |
| ***Rhode Island***<br><br>R.I. GEN. LAWS § 11-49.3-1 et seq. | Applies to municipal or state agencies or person that stores, owns, collects, processes, maintains, acquires, uses, or licenses data that includes ***personal information***, defined as an individual's first name or first initial and last name plus:<br>• SSN<br>• Driver's license number, Rhode Island identification card number, or tribal identification number.<br>• Account number, credit, or debit card number plus any required security code, access code, password, or personal identification number.<br>• Medical or health insurance information.<br>• E-mail address plus any required security code, access code, or password.<br><br>Does not include publicly available information that is lawfully made available to the | Requires written or electronic notice "in the most expedient time possible" not to exceed 45 days after confirmation of the breach.<br><br>Requires notice to include description of the incident, information subject to the breach, timing, remediation services offered including reporting agencies and the attorney general, and a description of how the consumer requests a security freeze.<br><br>If the breach requires notification of more than 500 affected individuals, requires notice to:<br>• Attorney General.<br>• Major credit reporting agencies. | In limited circumstances (i.e., if the cost of providing notice would exceed $25,000 or the affected class of subject persons to be notified exceeds 50,000), permits notice via email, conspicuous posting of the notice on the entity's website, and notification to major statewide media. | Exempts or deems compliant certain entities from the breach notification requirements, including:<br>• Entities subject to federal requirements on data breach notification (i.e., HIPAA, Federal Interagency Guidance).<br>• Entities that maintain their own notification procedures that are at least as thorough as these the requirements in the broad data breach notification law.<br><br>Deems sufficient for compliance notification requirements or security system breach procedures pursuant to requirements established by the | ***Penalties.*** Provides that each reckless violation is a civil violation which may incur a penalty of not more than $100 per record. Each violation that is knowing or willful may incur a penalty of $200 per record. |

| State | Covered Entities and Data | Method and Timing of Notice | Substitute Notice | Exceptions | Other |
|---|---|---|---|---|---|
| | general public from government records. | | | primary or functional state or federal regulator. | |
| ***South Carolina***<br><br>S.C. CODE § 39-1-90 | Applies to any person conducting business in the state that owns or license computerized data that includes ***personal information***, defined as the first name or first initial and last name plus:<br>• SSN<br>• Driver's license number or state identification card number issued instead of a driver's license.<br>• Financial account number, or credit card or debit card number plus any required security code, access code, or password.<br>• Other numbers or information which may be used to access a person's financial accounts or numbers or information issued by a governmental or regulatory entity that uniquely will identify an individual.<br><br>Does not include information lawfully obtained from publicly available information or from | Requires written, electronic, or telephonic notice "in the most expedient time possible and without unreasonable delay."<br><br>Requires notice to include description, information subject to the breach, date of breach, date discovered, remediation services including contact information, and a description of the consumer's ability to file or obtain a police report or security freeze.<br><br>If the breach requires notification of more than 1,000 affected individuals, requires notice to:<br>• Consumer Protection Division of the Department of Consumer Affairs.<br>• Consumer reporting agencies.<br><br>If a third-party (i.e., a "third party agent") experiences a breach, requires notification immediately following discovery. | In limited circumstances (i.e., if the cost of providing notice exceeds $25,000 or the affected class of subject persons to be notified exceeds 50,000) permits notice via email, conspicuous posting on the entity's website, and notification to major statewide media. | Exempts or deems compliant certain entities from the breach notification requirements, including:<br>• Entities subject to federal requirements on data breach notification (i.e., GLBA, Federal Interagency Guidance).<br>• Entities that maintain their own notification procedures that are at least as thorough as these the requirements in the broad data breach notification law. | ***Penalties.*** Provides that each knowing and willful violation is a civil violation which may incur a penalty of not more than $1,000 per record. |

| State | Covered Entities and Data | Method and Timing of Notice | Substitute Notice | Exceptions | Other |
|---|---|---|---|---|---|
| | government records lawfully made available to the general public. | | | | |
| ***South Dakota***<br><br>South Dakota Codified Laws § 22–40–19 et seq. | Applies to any person or business that conducts business in the state that owns or licenses computerized ***personal or protected information***, defined as a person's first name or first initial and last name plus:<br>• SSN<br>• Driver license number or other unique identification number created or collected by a government body.<br>• Account, credit card, or debit card number, plus any required security code, access code, password, routing number, or PIN.<br>• Health information as defined by federal law.<br>• Identification number assigned to a person by the person's employer plus any required security code, access code, password, or biometric data. | Requires written or electronic notice no later than 60 days following discovery of the breach.<br><br>Requires notification to consumer reporting agencies without unreasonable delay.<br><br>If the breach requires notification of more than 250 affected individuals, requires notice to the Attorney General. | In limited circumstances (i.e., the cost of providing notice would exceed $250,000, that the affected class of persons to be notified exceeds 500,000), permits notice via email, conspicuous posting on the information holder's website, and notification to statewide media. | Exempts or deems compliant certain entities from the breach notification requirements, including:<br>• Entities subject to federal requirements on data breach notification (i.e., GLBA, HIPAA).<br>• Entities that maintain their own notification procedures that are at least as thorough as these the requirements in the broad data breach notification law. | ***Penalties.*** Provides that the Attorney General may bring an action for civil penalties. |

| State | Covered Entities and Data | Method and Timing of Notice | Substitute Notice | Exceptions | Other |
|---|---|---|---|---|---|
| | Does not include information lawfully obtained from publicly available information or from government records lawfully made available to the general public. | | | | |
| ***Tennessee***<br><br>TENN. CODE § 47-18-2107 | Applies to any person or business that conducts business in the state that owns or licenses computerized data that includes ***personal information***, defined as an individual's first name or first initial and last name plus:<br>• SSN<br>• Driver license number.<br>• Account, credit card, or debit card number, plus any required security code, access code, or password.<br><br>Does not include information lawfully made available to the general public from federal, state, or local government records or information that has been redacted or otherwise made unusable. | Requires written or electronic notice immediately but not later than 45 days following discovery or notification.<br><br>If the breach requires notification of more than 1,000 affected individuals, requires notice to:<br>• Consumer reporting agencies.<br>• Credit bureaus.<br><br>If a third-party (i.e., a "third party agent") experiences a breach, requires owner notification within 45 days following discovery or notification. | In limited circumstances (i.e., the cost of providing notice would exceed $250,000 or that the affected class of subject persons to be notified exceeds 500,000 persons), permits notice via email, conspicuous posting on the website of the entity, and notification to major statewide media. | Exempts or deems compliant certain entities from the breach notification requirements, including:<br>• Entities subject to federal requirements on data breach notification (i.e., GLBA, HIPAA).<br>• Entities that maintain their own notification procedures that are at least as thorough as these the requirements in the broad data breach notification law. | ***Private Right of Action***. Provides that any customer of an information holder who is a person or business entity not an agency of the state who is injured may institute a civil action to recover damages and rejoin the information holder from further action in violation. |
| ***Texas***<br><br>TEX. BUS. & COM. CODE §§ 521.002, 521.053 | Applies to any person or entity that conducts business in the state and owns or licenses computerized data that includes | Requires written or electronic notice "without unreasonable delay" but not later than the 60th day after the date on which the | In limited circumstances (i.e., the cost of providing notice would exceed $250,000 or the | Exempts or deems compliant certain entities from the breach notification | ***Penalties.*** Provides that remedies include injunctive relief and civil penalties |

| State | Covered Entities and Data | Method and Timing of Notice | Substitute Notice | Exceptions | Other |
|---|---|---|---|---|---|
| | sensitive ***personal identifying information*** defined as:<br>• An individual's name.<br>• SSN<br>• Date of birth.<br>• Government-issued ID number.<br>• Mother's maiden name<br>• Biometric data.<br>• Unique electronic identification number, address, or routing code.<br>• Telecommunication access device.<br>• Account number or credit or debit card number plus required security code, access code, or password.<br><br>Also includes sensitive personal information that identifies an individual and relates to the physical or mental health or condition of the individual, the provision of health care to the individual, or payment for the provision of health care to the individual.<br><br>Sensitive personal information does not include publicly available information that is lawfully made available to the general public from the federal | person determines the breach occurred.<br><br>Permits notice to be in accordance with another state's notification requirement if the affected individual is a resident of another state.<br><br>If the breach requires notification of more than 10,000 affected individuals, requires notice to each consumer reporting agency.<br><br>If the breach requires notification of more than 250 residents, requires notification to the attorney general. | number of affected persons exceeds 500,000), permits notice via electronic mail, conspicuous posting of the notice on the person's website; or notice published in or broadcast on major statewide media. | requirements, including:<br>• Entities that maintain their own notification procedures that are at least as thorough as these the requirements in the broad data breach notification law. | of at least $2,000 but not more than $50,000 for each violation. Provides that civil penalties for failure to comply may incur $100 per person to whom notification was due per day not to exceed $250,000 per breach. |

| State | Covered Entities and Data | Method and Timing of Notice | Substitute Notice | Exceptions | Other |
|---|---|---|---|---|---|
| | government or a state or local government. | | | | |
| ***Utah***<br><br>UTAH CODE §§ 13-44-101, 13-44-202, 13-44-301 | Applies to any person who conducts business in the state and owns or licenses ***personal information*** defined as a person's first name or first initial and last name plus:<br>• SSN<br>• Financial account number, or credit or debit card number plus required security code, access code, or password.<br>• Driver license number or state identification card number.<br><br>Does not include information contained in federal, state, or local government records or in widely distributed media lawfully made available to the general public. | Requires notice in "the most expedient time possible without unreasonable delay" not to exceed 45 days via written (first class mail), telephonic, or electronic methods.<br><br>If a third-party (i.e., a "third party agent") experiences a breach, requires owner notification immediately following discovery. | In limited circumstances (i.e., if required notice is "not feasible"), permits notice via publishing notice of the breach in a newspaper of general circulation in the state. | Exempts or deems compliant certain entities from the breach notification requirements, including:<br>• Entities that maintain their own notification procedures that are at least as thorough as these the requirements in the broad data breach notification law.<br>• Financial institutions or affiliates of financial institutions as defined in 15 U.S.C. § 6809.<br><br>Deems sufficient for compliance notification requirements or security system breach procedures pursuant to requirements established by the primary or functional | ***Penalties.*** Provides that violators are subject to a civil fine of no more than $2,500 for a violation or series of violations concerning a specific consumer and no more than $100,000 in the aggregate for violations concerning more than one consumer. This penalty does not apply if the violations concern more than 10,000 Utah residents and more than 10,000 residents of other states or if the entity agrees to settle for a greater amount.<br><br>***Waivers.*** Provides that waivers are void/unenforceable . |

| State | Covered Entities and Data | Method and Timing of Notice | Substitute Notice | Exceptions | Other |
|---|---|---|---|---|---|
| | | | | state or federal regulator. | |
| ***Vermont***<br><br>9 V.S.A. §§ 2430, 2435 | Applies to any data collector and any entity that handles, collects, disseminates, or otherwise deals with or that owns or licenses computerized nonpublic ***personal information*** defined as an individuals first name or first initial plus:<br>• SSN<br>• Driver license or nondriver State identification card number, individual TIN, passport number, military identification card number, or other identification card number that originates from a government identification document that is commonly used to verify identity for a commercial transaction.<br>• Financial account number, credit card number, or debit card number if the number could be used without additional identifying information, access codes, or passwords. | Requires notice via written, telephonic, or electronic notice "in the most expedient time possible and without unreasonable delay" but not later than 45 days after discovery of the breach.<br><br>Requires notice to include the incident in general terms, the type of information subject to breach, general acts of the data collector to protect the information from further breach, telephone number that the consumer may call for assistance and information, advice that directs the consumer to remain vigilant, and the approximate date of the security breach.<br><br>Also requires notice to the Attorney General or to the Department of Financial Regulation.<br><br>Requires notification to consumer reporting agencies if notice must be made to more than 1,000 consumers at one time.<br><br>If a third-party (i.e., a "third party agent") experiences a | In limited circumstances (i.e., the cost would exceed $10,000), permits notice via conspicuous posting of the notice on the entity's website and notification to major statewide and regional media. | Exempts or deems compliant certain entities from the breach notification requirements, including:<br>• Entities subject to federal requirements on data breach notification (i.e., HIPAA, Federal Interagency Guidance). | ***Waivers.*** Provides that waivers are void/unenforceable. |

| State | Covered Entities and Data | Method and Timing of Notice | Substitute Notice | Exceptions | Other |
|---|---|---|---|---|---|
| | • A password, personal identification number, or other access code for a financial account.<br>• Biometric data.<br>• Genetic information.<br>• Health records or records of a wellness program or similar program of health promotion or disease prevention, a health care professional's medical diagnose or treatment of the consumer, or a health insurance policy number.<br><br>Does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. | breach, requires owner notification immediately following discovery. | | | |
| ***Virginia***<br><br>VA. CODE § 18.2-186.6; § 32.1-127.1:05; amendment to § 18.2-186.6; H.B. 2396 | Applies to any individual or entity that owns or licenses computerized data that includes ***personal information*** defined as an individual's first name or first initial and last name plus:<br>• SSN<br>• Driver's license number or state | Requires written, telephonic, or electronic notice "without unreasonable delay[.]"<br><br>Requires notice to include a description of the incident, the type of information subject to unauthorized access, general acts taken to protect the information from further unauthorized access, a telephone number the | In limited circumstances (i.e., the cost of providing notice will exceed $50,000 or the affected class of Virginia residents to be notified exceeds 100,000 residents), permits notice via email, conspicuous posting of | Exempts or deems compliant certain entities from the breach notification requirements, including:<br>• Entities subject to federal requirements on data breach | ***Penalties.*** Provides that the Attorney General may impose a civil penalty not to exceed $150,000 per breach of the system or series of breaches discovered in a |

| State | Covered Entities and Data | Method and Timing of Notice | Substitute Notice | Exceptions | Other |
|---|---|---|---|---|---|
| | identification card number.<br>• Financial account number, or credit card or debit card number, plus any required security code, access code, or password.<br>• Passport number.<br>• Military identification number.<br><br>Does not include information lawfully obtained from publicly available information or from federal, state, or local government records lawfully made available to the general public. | person may call for further information and assistance if one exists, and advice directing the person to remain vigilant.<br><br>If a third-party (i.e., a "third party agent") experiences a breach, requires owner notification.<br><br>Requires notification to the Attorney General. If notice to more than 1,000 individuals is required, requires notification to the Attorney General to include timing, distribution, and content of the notice. | the notice on the website of the individual or entity, and notice to statewide media. | notification (i.e., GLBA, HIPAA).<br>• Entities that maintain their own notification procedures that are at least as thorough as these the requirements in the broad data breach notification law. | single investigation. |
| ***Washington***<br><br>WASH. REV. CODE § 19.255.010 et seq., § 42.56.590 | Applies to any person or business that owns or licenses data including ***personal information*** defined as an individual's first name or first initial and last name plus:<br>• SSN<br>• Driver's license number or Washington identification card number.<br>• Account number or credit or debit card number plus any required security code, access code, or | Requires written or electronic notice "in the most expedient time possible, without unreasonable delay" but not more than 30 days after discovery of the breach.<br><br>Requires notice to include name and contact information of reporting person or business, list of types of personal information believed to have been subject of the breach, timeframe of exposure, and toll-free number and address of major credit reporting agencies. | In limited circumstances (i.e., the cost of providing notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000), permits notice via email, conspicuous posting of the notice on the entity's website, and notification to major statewide media. | Exempts or deems compliant certain entities from the breach notification requirements, including:<br>• Entities subject to federal requirements on data breach notification (i.e., HIPAA).<br>• Entities that maintain their own notification procedures that | |

| State | Covered Entities and Data | Method and Timing of Notice | Substitute Notice | Exceptions | Other |
|---|---|---|---|---|---|
| | password or any other numbers or information that can be used to access a person's financial account.<br>• Full date of birth.<br>• Private key that is unique to an individual and that is used to authenticate or sign an electronic record.<br>• Student, military, or passport identification number.<br>• Health insurance policy number or health insurance identification number.<br>• Any information about a consumer's medical history or mental or physical condition or about a health care professional's medical diagnosis or treatment of the consumer.<br>• Biometric data.<br>• User name or email address plus password or security questions and answers.<br><br>Does not include publicly available information that is lawfully made available to the | Requires notification to the Attorney General if notification to more than 500 residents as a result of a single breach along with electronic sample of notification, number or estimate of consumers affected, timeframe of exposure, and summary of steps taken to contain.<br><br>If a third-party (i.e., a "third party agent") experiences a breach, requires owner notification immediately following discovery. | | are at least as thorough as these the requirements in the broad data breach notification law.<br>• Financial institutions as defined by federal law (i.e., under authority of the Office of the Comptroller of the Currency, the FDIC, the NCUA, or the Federal Reserve). | |

| State | Covered Entities and Data | Method and Timing of Notice | Substitute Notice | Exceptions | Other |
|---|---|---|---|---|---|
| | general public from federal, state, or local government records. | | | | |
| ***West Virginia***<br><br>W. VA. CODE § 46A-2A-101 et seq. | Applies to any individual or business entity that owns or licenses computerized data that includes ***personal information*** defined as the first name or first initial and last name plus:<br>• SSN<br>• Driver's license number or state identification card number issued in lieu of a driver's license.<br>• Financial account number, or credit card, or debit card number plus required security code, access code or password.<br><br>Does 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. | Requires notice "without unreasonable delay" via written, telephonic, or electronic method.<br><br>Requires notice to include a description of the categories of information believed to have been accessed, a telephone number or website the individual may use to contact the entity and learn what types of information maintained, and toll-free contact telephone number and addresses for the major credit reporting agencies and how to place fraud alert or security freeze.<br><br>Requires notification to consumer reporting agencies if notice must be made to more than 1,000 consumers at one time.<br><br>If a third-party (i.e., a "third party agent") experiences a breach, requires owner notification immediately following discovery. | In limited circumstances (i.e., the cost of providing notice will exceed $50,000 or that the affected class of residents to be notified exceeds 100,000 persons), permits notice via email, conspicuous posting of the notice on the entity's website, or notice to major statewide media. | Exempts or deems compliant certain entities from the breach notification requirements, including:<br>• Entities subject to federal requirements on data breach notification (i.e., Federal Interagency Guidance).<br>• Entities that maintain their own notification procedures that are at least as thorough as these the requirements in the broad data breach notification law. | N/A |
| ***Wisconsin*** | Applies to any entity that maintains or licenses ***personal information*** defined as an | Requires notice via mail or previously used method "within a reasonable time" but not | In limited circumstances (i.e., if the entity cannot with | Exempts or deems compliant certain entities from the | |

| State | Covered Entities and Data | Method and Timing of Notice | Substitute Notice | Exceptions | Other |
|---|---|---|---|---|---|
| WIS. STAT. § 134.98 | individual's last name and the individual's first name or first initial plus:<br>• SSN<br>• The individual's driver's license number or state identification number.<br>• The number of the individual's financial account number, including a credit or debit card account number, or any security code, access code, or password.<br>• The individual's deoxyribonucleic acid profile.<br>• Biometric data.<br><br>Does not include publicly available information lawfully made widely available through media or lawfully made available to the general public from federal, state, or local government records or disclosures to the general public required by law. | exceeding 45 days after learning of the breach.<br><br>Requires notification to consumer reporting agencies if notice must be made to more than 1,000 consumers at one time.<br><br>If a third-party (i.e., a "third party agent") experiences a breach, requires owner notification immediately following discovery. | reasonable diligence determine the mailing address), permits notice via a method reasonably calculated to provide actual notice. | breach notification requirements, including:<br>• Entities subject to federal requirements on data breach notification, (i.e. entities covered under GLBA, HIPAA). | N/A |
| ***Wyoming***<br><br>WYO. STAT. § 40-12-501 et seq. | Applies to an individual or entity that conducts business in the state and owns or licenses computerized data that includes ***personal identifying information*** defined as an individual's last name and the | Requires notice "in the most expedient time possible and without unreasonable delay" via written or electronic methods.<br><br>Requires notice to include a toll-free number that the individual | In limited circumstances (i.e., the cost of providing notice would exceed $10,000.00 for Wyoming-based persons or businesses | Exempts or deems compliant certain entities from the breach notification requirements, including: | ***Penalties.*** Provides that the Attorney General may bring an action to address violations and for other relief that |

| State | Covered Entities and Data | Method and Timing of Notice | Substitute Notice | Exceptions | Other |
|---|---|---|---|---|---|
| | individual's first name or first initial plus:<br>• SSN<br>• Driver license number.<br>• Account number or credit card number or debit card number plus any security code, access code, or password.<br>• Tribal identification card.<br>• Federal or state government-issued identification card.<br>• Shared secrets or security tokens.<br>• Username or email address plus password or security question and answer.<br>• Birth or marriage certificate.<br>• Medical information.<br>• Health insurance information.<br>• Biometric data.<br>• Individual TIN.<br><br>Does not include information contained in federal, state, or local government records or in widely distributed media lawfully made available to the general public. | may use to contact the person collecting data and from which the individual may learn contact numbers and addresses for the major credit reporting agencies, types of personal information reasonably believed to have been the subject of the breach, actions taken to protect the system from further breaches, advice that directs the person to remain vigilant, whether notification has been delayed.<br><br>If a third-party (i.e., a "third party agent") experiences a breach, requires owner notification immediately following discovery. | or $250,000 for all others or that the affected class of persons exceeds 10,000 for Wyoming-based persons or 500,000 for all others), permits notice via conspicuous posting of the notice on the internet and notification to major statewide media. | • Entities subject to federal requirements on data breach notification, (i.e., entities covered under HIPAA).<br>• Certain financial institutions as defined in 15 U.S.C. § 6809 and 12 U.S.C. § 1752. | may be appropriate to ensure compliance or to recover damages or both. |