Clausen Miller PC

50 State Survey: Data Breach Notification Statutes

Clausen Miller P.C.

www.clausen.com

50 State Survey: Data Breach Notification Statutes

Updated: September 2014

Please keep in mind that this guide is intended only as a quick reference tool and a source of general information. It is not intended, nor should it be considered, the rendition of legal advice. In specific cases, it is always important to consult counsel regarding the rules of the court within which you are practicing and the pertinent case law.

Should you be interested in information about Clausen Miller P.C.'s data breach security practice group, please contact Thomas H. Ryerson at tryerson@clausen.com.

Clausen Miller P.C. thanks attorneys Thomas Ryerson, Mindy Medley, Scott Shinkan and law student and Aleksia Culafic for their contributions to this survey.

TABLE OF CONTENTS

* No Statute Designated

* No Statute Designated

* No Statute Designated

ALASKA

ALASKA STAT. § 45.48.090 *et seq*.

What is a data breach?

"Breach of the security" means the unauthorized acquisition, or reasonable belief of unauthorized acquisition, of personal information that compromises the security, confidentiality, or integrity of the personal information maintained by the information collector. "Acquisition" includes acquisition by (A) photocopying, facsimile, or other paper-based method; (B) a device, including a computer, that can read, write, or store information that is represented in numerical form; or (C) a method not identified by (A) or (B).

Who does this law apply to?

Any covered person who owns or licenses personal information in any form that includes personal information on a state resident. "Covered person" means a (A) person doing business; (B) governmental agency; or (C) person with more than 10 employees.

Who must be notified?

If a covered person owns or licenses personal information in any form that includes personal information on a state resident, and a breach of the security of the information system that contains personal information occurs, the covered person shall, after discovering or being notified of the breach, disclose the breach to each state resident whose personal information was subject to the breach.

If an information collector is required to notify more than 1,000 state residents of a breach, the information collector shall also notify all consumer credit reporting agencies that compile and maintain files on consumers on a nationwide basis and provide the agencies with the timing, distribution, and content of the notices to state residents.

When must they be notified?

An information collector shall make the disclosure required in the most expeditious time possible and without unreasonable delay, except as provided in AS 45.48.020 and as necessary to determine the scope of the breach and restore the reasonable integrity of the information system.

What must be included in the notification?

The content of the notification is not explicitly addressed in the statute.

How must they be notified?

An information collector shall make the disclosure by (1) a written document sent to the most recent address the information collector has for the state resident; (2) electronic means if the information collector's primary method of communication with the state resident is by electronic means or if making the disclosure by the electronic means is consistent with the provisions regarding electronic records and signatures required for notices legally required to be in writing under 15 U.S.C. 7001 *et seq.*; or (3) if the information collector demonstrates that the cost of providing notice would exceed $150,000, that the affected class of state residents to be notified exceeds 300,000, or that the information collector does not have sufficient contact information to provide notice, by (A) electronic mail if the information collector has an electronic mail address for the state resident; (B) conspicuously posting the disclosure on the

Internet website of the information collector if the information collector maintains an Internet website; or by (C) providing notice to major statewide media.

Do any exceptions or exemptions apply?

An information collector may delay disclosing the breach if an appropriate law enforcement agency determines that disclosing the breach will interfere with a criminal investigation. However, the information collector shall disclose the breach to the state resident in the most expeditious time possible and without unreasonable delay after the law enforcement agency informs the information collector in writing that disclosure of the breach will no longer interfere with the investigation.

What are the legal consequences for violating the law?

If an information collector who is a governmental agency violates this statute, the information collector is liable to the state for a civil penalty of up to $500 for each state resident who was not notified, but the total civil penalty may not exceed $50,000. The governmental agency may be enjoined from further violations. The Department of Administration may enforce this section against a governmental agency.

If an information collector who is not a governmental agency violates the statute, the violation is an unfair or deceptive act or practice under AS 45.50.471 -- 45.50.561. However, the information collector is not subject to the civil penalties imposed under AS 45.50.551 but is liable to the state for a civil penalty of up to $500 for each state resident who was not notified, except that the total civil penalty may not exceed $50,000. Damages that may be awarded against the information collector are limited to actual economic damages that do not exceed $500; and (B) AS 45.50.537 are limited to actual economic damages.

ARIZONA

A.R.S. § 44-7501 *et seq*.

What is a data breach?

"Breach", "breach of the security of the system", "breach of the security system" or "security breach" means an unauthorized acquisition of and access to unencrypted or unredacted computerized data that materially compromises the security or confidentiality of personal information maintained by a person as part of a database of personal information regarding multiple individuals and that causes or is reasonably likely to cause substantial economic loss to an individual.

Good faith acquisition of personal information by an employee or agent of the person for the purposes of the person is not a breach of the security system if the personal information is not used for a purpose unrelated to the person or subject to further wilful unauthorized disclosure.

Who does this law apply to?

When a person that conducts business in the state and that owns or licenses unencrypted computerized data that includes personal information becomes aware of an incident of unauthorized acquisition and access to unencrypted or unredacted computerized data that includes an individual's personal information, the person shall conduct a reasonable investigation to promptly determine if there has been a breach of the security system.

A person that maintains unencrypted computerized data that includes personal information that the person does not own shall notify and cooperate with the owner or the licensee of the information of any breach of the security of the system following discovery of the breach without unreasonable delay. Cooperation shall include sharing information relevant to the breach of the security of the system with the owner or licensee. The person that owns or licenses the computerized data shall provide notice to the individual pursuant to this section. The person that maintained the data under an agreement with the owner or licensee is not required to provide notice to the individual pursuant to this section unless the agreement stipulates otherwise.

Who must be notified?

A person that conducts business in this state and that owns or licenses unencrypted computerized data that includes personal information who determines that there has been a breach in the security system shall notify affected individuals.

A person that maintains unencrypted computerized data that includes personal information that the person does not own shall notify and cooperate with the owner or the licensee of the information of any breach of the security of the system following discovery of the breach without unreasonable delay.

When must they be notified?

The notice shall be made in the most expedient manner possible and without unreasonable delay subject to the needs of law enforcement and any measures necessary to determine the nature and scope of the breach, to identify the individuals affected or to restore the reasonable integrity of the data system.

What must be included in the notification?

The content of the notification is not explicitly addressed in the statute.

How must they be notified?

Disclosure required under this section shall be provided by one of the following methods: (1) written notice; (2) electronic notice if the person's primary method of communication with the individual is by electronic means or is consistent with the provisions regarding electronic records and signatures set forth in the electronic signatures in global and national commerce act; (3) telephonic notice; or (4) substitute notice if the person demonstrates that the cost of providing notice would exceed fifty thousand dollars or that the affected class of subject individuals to be notified exceeds one hundred thousand persons, or the person does not have sufficient contact information.

Substitute notice shall consist of (1) electronic mail notice if the person has electronic mail addresses for the individuals subject to the notice; (2) conspicuous posting of the notice on the web site of the person if the person maintains one; and (3) notification to major statewide media.

Do any exceptions or exemptions apply?

The notification required by this section may be delayed if a law enforcement agency advises the person that the notification will impede a criminal investigation. The person shall make the notification after the law enforcement agency determines that it will not compromise the investigation.

A person who maintains the person's own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the requirements of this section shall be deemed to be in compliance with the notification requirements of this section if the person notifies subject individuals in accordance with the person's policies if a breach of the security system occurs.

A person that complies with the notification requirements or security breach procedures pursuant to the rules, regulations, procedures, guidance or guidelines established by the person's primary or functional federal regulator is deemed to be in compliance with this section.

A person is not required to disclose a breach of the security of the system if the person or a law enforcement agency, after a reasonable investigation, determines that a breach of the security of the system has not occurred or is not reasonably likely to occur.

What are the legal consequences for violating the law?

This section may only be enforced by the attorney general. The attorney general may bring an action to obtain actual damages for a wilful and knowing violation of this section and a civil penalty not to exceed ten thousand dollars per breach of the security of the system or series of breaches of a similar nature that are discovered in a single investigation.

ARKANSAS

ARK. CODE ANN. § 4-110-101 *et seq*.

What is a data breach?

A data breach is any unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person or business.

Who does this law apply to?

Any person or business that acquires, owns, or licenses computerized data that includes personal information.

A business means a sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not organized to operate at a profit, including financial institutions organized, chartered, or holding a license or authorization certificate under the law of any state or country.

Who must be notified?

Following the discovery or notification of a data breach any resident of Arkansas whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person must be notified of the breach.

When must they be notified?

The notification must be sent out in the most expedient time and manner possible without unreasonable delay. A reasonable delay to wait to notify consists of police investigation and the time needed to determine the scope of the breach and to restore the reasonable integrity of the data system.

What must be included in the notification?

The content of the notification is not explicitly addressed in the statute.

How must they be notified?

Notice must be sent in a written form or through electronic mail that is consistent with the provisions of 15 U.S.C § 7001 regarding electronic records and signatures.

Do any exceptions or exemptions apply?

If a person or business has its own procedures, it shall be deemed to be in compliance with the notification requirements if the notification is in accordance with the person or businesses' policies in the event of a data breach.

If a law enforcement agency determines that the notification will impede a criminal investigation, the notification can be delayed.

If after a reasonable investigation it is determined there was no reasonable likelihood of harm to the customers, no notification is required.

What are the legal consequences for violating the law?

If a person or business violates the law, it is punishable by action of the Attorney General under Chapter 88 of the Deceptive Trade Practices Act.

CALIFORNIA

CAL. CIV. CODE § 1798.29; 1798.80 *et seq.*

What is a data breach?

A data breach is any unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information.

Who does this law apply to?

Any person or business that conducts business in California, and owns or licenses computerized data that includes personal information.

A business is a sole proprietorship, partnership, corporation, association, or other group, however organized under the law of any state or country.

Who must be notified?

Following the discovery or notification of a data breach, the person or business must notify every California resident whose personal information was or was reasonably believed to have been acquired by an unauthorized person.

When must they be notified?

The notification must be sent in the most expedient time possible and without unreasonable delay. Reasonable delays include steps necessary to determine the scope of the breach and steps to restore the reasonable integrity of the data system.

If the breach consists of more than 500 people, the person or business must submit a copy of the notification to the attorney general.

What must be included in the notification?

The notification must be written in plain language and include 1) the contact information of the person or business that experienced the data breach; 2) a list of the types of personal information that were or are reasonably believed to be the subject of the breach; 3) the date of the

breach (can be estimated date of breach or a range of dates within which the breach occurred if exact date is not known); 4) whether the notification was delayed because of law enforcement investigation; 5) a general description of the breach; and 6) a toll free number and address for the major credit reporting agencies if the breach exposed a social security number or driver's license number.

The person or business has the option to include information about what has been done to protect individuals whose information has been disclosed or advise on what steps can be taken by the individual to protect him or herself.

How should they be notified?

Notice must be sent in a written form or through electronic mail that is consistent with the provisions of 15 U.S.C § 7001 regarding electronic records and signatures.

Do any exceptions or exemptions apply?

The notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation.

If the person or business maintains their own notification policies for data breach, the notification requirements will be fulfilled if the notification follows the policies created by the person or business. The notification must still be sent in a timely manner.

What are the legal consequences for violating the law?

Any customer injured by a violation of this statue my institute a civil action.

COLORADO

COLO. REV. STAT. ANN. § 6-1-716 (2006); as amended (2010).

What is a data breach?

"Breach of the security of the system" means the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an individual or a commercial entity.

Who does this law apply to?

Any individual or commercial entity that conducts business in Colorado and owns, licenses, or maintains computerized data that includes personal information comes within the purview of this statute. Upon becoming aware of the breach, the individual or commercial entity must conduct a prompt investigation in good faith to determine the likelihood that personal information has been or will be misused.

Notification is not required if after a good faith, prompt and reasonable investigation, the entity determines that misuse of personal information about a Colorado resident has not occurred and is not likely to occur.

Who must be notified?

The individual or the commercial entity shall give notice as soon as possible to the affected Colorado resident unless the investigation determines that the misuse of information about a Colorado resident has not occurred and is not reasonably likely to occur.

If an individual or commercial entity is required to notify more than 1,000 Colorado residents of a breach of the security of the system, the individual or commercial entity must also notify, without unreasonable delay, all consumer reporting agencies.

When must they be notified?

If misuse of personal information is likely to occur, notice must be given as soon as possible to the Colorado resident when the individual or commercial entity becomes aware of a breach of the security of the system. Notice must be given without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of breach and to restore the reasonable integrity of the system.

What must be included in the notification?

The content of the notification is not explicitly addressed in the statute.

How must they be notified?

Notice must be provided by: (1) written notice to the postal address listed in the records of the individual or commercial entity; (2) telephonic notice; (3) electronic notice, if a primary means of communication is by electronic means or the notice provided is consistent with federal electronic signature laws; or (4) substitute notice if: (i) the cost of notice will exceed $250,000; (ii) the affected class of persons exceeds 250,000 Colorado residents; or (iii) the individual or commercial entity does not have sufficient contact information.

Do any exceptions or exemptions apply?

An individual or commercial entity that maintains its own notification procedures as part of an information security policy for the treatment of personal information and whose procedures are otherwise consistent with the timing requirements of this section is in compliance with this statute if the individual or commercial entity notifies affected Colorado customers in accordance with its policies in the event of a breach.

In addition, required notification may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation. As soon as the law enforcement agency determines that notification will no longer impede the investigation, the individual or commercial entity is required to provide notice without unreasonable delay.

What are the legal consequences for violating the law?

The attorney general may bring an action to address violations of this section and for other relief that may be appropriate to ensure compliance with the law.

CONNECTICUT

CONN. GEN. STAT. ANN. § 36a-701b

What is a data breach?

"Breach of security" means unauthorized access to or unauthorized acquisition of electronic files, media, databases, or computerized data containing personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable.

Who does this law apply to?

This law applies to any person who conducts business in Connecticut, and who, in the ordinary course of such person's business, owns, licenses or maintains computerized data that includes personal information. Those subject to this statute must provide notice of any breach of security following the discovery of the breach.

Notice is not required if, after an appropriate investigation and consultation with relevant federal, state and local agencies responsible for law enforcement, the person reasonably determines that the breach will not likely result in harm to the individuals whose personal information has been acquired and accessed.

Who must be notified?

Notice of data security breaches must be provided to any resident of Connecticut whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person through the breach of security.

When notice of breach of security is provided to the resident, notice must also be given to the attorney general.

When must they be notified?

Notice must be given immediately following the discovery, if the personal information was, or is reasonably believed to have been, accessed by an unauthorized person.

The notice must be made without unreasonable delay, consistent with any measures necessary to determine the nature and scope of the breach, to identify individuals affected, or to restore the reasonable integrity of the data system.

This requirement is subject to delay for a reasonable period of time at the request of a law enforcement agency, as well as for the completion of an investigation to determine the nature and scope of the incident, to identify the individuals affected, or to restore the reasonable integrity of the data system.

What must be included in the notification?

The content of the notification is not explicitly addressed in the statute.

How must they be notified?

Notice to a resident, owner or licensee must be provided by written notice, telephonic notice, or electronic notice, provided such notice is consistent with federal law. Substitute notice is also permitted if it is shown that the cost of providing notice would exceed $250,000, that the affected class of subject persons to be notified exceeds 500,000 persons, or that the person does not have sufficient contact information.

Do any exceptions or exemptions apply?

If notice is required and is delayed due to law enforcement concerns, it must be given after the law enforcement agency determines that notification will not compromise the criminal investigation and so notifies the person of such determination.

A business that maintains its own security breach procedures as part of an information security policy for the treatment of personal information and otherwise complies with the timing requirements of this law, is in compliance with the security breach notification requirements of

Connecticut if the business complies with its policy, and if notice is required, notice is also simultaneously given to the attorney general.

What are the legal consequences for violating the law?

Failure to comply with the law is considered an unfair trade practice for purposes of Section 42-110b of Connecticut's general statutes and will be enforced by the attorney general. The attorney general may seek direct damages and injunctive relief.

DELAWARE

DEL. CODE ANN. TIT. 6 § 12B-101 *et seq*.

What is a data breach?

"Breach of the security of the system" means the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an individual or a commercial entity.

Who does this law apply to?

This law applies to any commercial entity doing business in the state that owns or licenses computerized personal information about a state resident. When the business becomes aware of a breach of security of the data system, the business must conduct a good faith, reasonable, prompt investigation to determine the likelihood that the personal information has been or will be misused. Notice is not required if the entity determines that there is no reasonable likelihood of harm to consumers after a good-faith, reasonable, and prompt investigation.

Who must be notified?

If the investigation shows that such misuse has occurred or is likely to occur, the business must give notice to the affected state resident as soon as possible.

When must they be notified?

The notice must be given in the most expedient time possible, without unreasonable delay, consistent with legitimate law enforcement needs and any measures needed to determine the scope of the breach and to restore the reasonable integrity of the data system. Notice may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation.

What must be included in the notification?

The content of the notification is not explicitly addressed in the statute.

How must they be notified?

The Delaware statute allows for written notice, telephonic notice, and electronic notice that is consistent with 15 U.S.C. § 7001. Substitute notice is only permitted if the commercial entity demonstrates that the cost of providing the notice will exceed $75,000, that the number of state residents to be notified exceeds 100,000, or that the commercial entity does not have sufficient contact information to provide the notice.

Do any exceptions or exemptions apply?

If an individual or commercial entity maintains its own notification procedures as part of an information security policy for the treatment of personal information that is otherwise consistent with the timing requirements of this law, compliance with that policy is deemed to be compliance with the notice requirements of this law.

If an entity that is regulated by state or federal law that provides greater protection to personal information than that provided by this law, then compliance with that state or federal law is deemed to be compliant with this law. This exception does not relieve an individual or a commercial entity from a duty to comply with other requirements of state and federal law regarding the protection and privacy of personal information.

What are the legal consequences for violating the law?

Any affected Delaware resident can bring an action to recover damages that result from a violation of this law. Reasonable attorneys' fees are also recoverable. Additionally, the Delaware attorney general may bring an action in law, or equity, to address violations of this law and for other relief that may be appropriate. Violations of this law are also enforceable by the Consumer Protection Division of the Department of Justice.

DISTRICT OF COLUMBIA

D.C. CODE § 28-3851 *et seq*.

What is a data breach?

A "breach of the security of the system" is an unauthorized acquisition of computerized or other electronic data, or any equipment or device storing such data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. A good faith acquisition of personal information by an employee or agent is allowed under this statute if the personal information is not used improperly or subject to further unauthorized disclosure. Further, the acquisition of data that has been rendered secure, so as to be unusable by an unauthorized third party, shall not be deemed to be a breach of the security of the system.

Who does the law apply to?

Any person or entity who conducts business in the District of Columbia, and who, in the course of such business, owns or licenses computerized or other electronic data that includes personal information, and any person or entity who maintains, handles, or otherwise possesses computerized or other electronic data that includes personal information that the person or entity does not own.

Who must be notified?

Any person or entity who conducts business in the District of Columbia, and who owns or licenses computerized or other electronic data that includes personal information, shall promptly notify any District of Columbia resident whose personal information was included in the breach. Any person or entity who maintains, handles, or otherwise possesses computerized or other electronic data that includes personal information that the person or entity does not own shall notify the owner or licensee of the information.

If more than 1,000 persons must be notified, the person or entity shall also notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by section 603(p) of the Fair Credit Reporting Act, of the timing, distribution, and content of the notices.

When must they be notified?

The notification shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

What must be included in the notification?

The content of the notification is not explicitly addressed in the statute.

How must they be notified?

Notification may occur through written notice; electronic notice, if the customer has consented to receipt of electronic notice consistent with the provisions regarding electronic records and signatures set forth in the Electronic Signatures in Global and National Commerce Act; or substitute notice, if the person or business demonstrates that the cost of providing notice to persons subject to this subchapter would exceed $50,000, that the number of persons to receive notice under this subchapter exceeds 100,000, or that the person or business does not have sufficient contact information.

Substitute notice consists of e-mail notice when the person or business has an e-mail address for the subject persons; conspicuous posting of the notice on the website page of the person or business if the person or business maintains one; and notice to major local and, if applicable, national media.

Do any exceptions or exemptions apply?

Notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. Notice shall be made as soon as possible after the law enforcement agency determines that the notification will not compromise the investigation.

A person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this subchapter shall be deemed to be in compliance with the notification requirements if the person or business provides notice, in accordance with its policies, reasonably calculated to give actual notice to persons to whom notice is otherwise required to be given under this statute.

What are the legal consequences for violating the law?

Any District of Columbia resident injured by a violation of this subchapter may institute a civil action to recover actual damages, the costs of the action, and reasonable attorney's fees.

The attorney general may petition the Superior Court of the District of Columbia for temporary or permanent injunctive relief and for an award of restitution for property lost or damages suffered by District of Columbia residents as a consequence of the violation. The attorney general may recover a civil penalty not to exceed $100 for each violation, the costs of the action, and reasonable attorney's fees. Each failure to provide a District of Columbia resident with proper notification constitutes a separate violation.

FLORIDA

FL. STAT. ANN. § 501.171

What is a data breach?

"Breach of security" means unauthorized access of data in electronic form containing personal information. Good faith access of personal information by an employee or agent of the covered entity does not constitute a breach of security, provided that the information is not used for a purpose unrelated to the business or subject to further unauthorized use.

Who does this law apply to?

Each covered entity, governmental entity, or third-party agent shall take reasonable measures to protect and secure data in electronic form containing personal information. "Covered entity" means a sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity that acquires, maintains, stores, or uses personal information.

Notice is not required if, after an appropriate investigation and consultation with relevant federal, state, or local law enforcement agencies, the entity determines that the breach has not and will not likely result in identity theft or any other financial harm to the individuals whose personal information has been accessed. Even in such a scenario, the covered entity must still provide a written determination to the Florida Legal Affairs Department within 30 days of the covered entity's decision that no notice to individuals is required.

Who must be notified?

Notice must be provided to each individual in Florida whose personal information was, or is reasonably believed to have been, accessed as a result of the breach. A covered entity must provide notice to the Department of Affairs of any breach of security affecting 500 or more individuals in this state. If more than 1,000 individuals must be notified at a single time, the covered entity must also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in the Fair Credit Reporting Act.

When must they be notified?

Notice to individuals should be made as expeditiously as possible and without unreasonable delay, taking into account the time necessary for the entity to determine the scope of the breach of security, to identify individuals affected by the breach, and to restore the reasonable integrity of the data system that was breached, but no later than 30 days after the determination of a breach or reason to believe a breach occurred unless subject to a delay authorized.

What must be included in the notification?

The content of the notification is not explicitly addressed in the statute.

How must they be notified?

Notice to an affected individual must be written and sent to the mailing address of the individual in the records of the covered entity or emailed to the e-mail address of the individual in the records of the covered entity. A covered entity required to provide notice to an individual

may provide substitute notice if the cost of providing notice would exceed $250,000, if the affected individuals exceed 500,000 persons, or if the covered entity does not have an e-mail address or mailing address for the affected individuals.

Do any exceptions or exemptions apply?

If a federal, state, or local law enforcement agency determines that notice to individuals required would interfere with a criminal investigation, the notice may be delayed upon the written request of the law enforcement agency for a specified period that the law enforcement agency determines is reasonably necessary.

Notice provided pursuant to rules, regulations, procedures, or guidelines established by the covered entity's primary or functional federal regulator is deemed to be in compliance with the notice requirement in this subsection if the covered entity notifies affected individuals in accordance with the rules, regulations, procedures, or guidelines established by the primary or functional federal regulator in the event of a breach of security.

What are the legal consequences for violating the law?

This statute does not create a private cause of action. Instead, these provisions authorize the Florida Department of Legal Affairs to bring an enforcement action against an entity that commits any violation of the statutory notice requirements. Failure to provide adequate notice is deemed a violation of the Florida Deceptive and Unfair Trade Practices Act (FDUTPA) and is subject to following civil penalties: $1,000 per day for the first 30 days, $50,000 thereafter for each 30-day period or portion thereof for up to 180 days, or $500,000 as the maximum amount of total penalties for violations continuing more than 180 days.

GEORGIA

GA. CODE ANN., § 10-1-911 *et seq*.

What is a data breach?

"Breach of the security of the system" means unauthorized acquisition of an individual's electronic data that compromises the security, confidentiality, or integrity of personal information of such individual maintained by an information broker or data collector.

Who does this law apply to?

This law applies to any information broker or data collector that maintains computerized data including the personal information of individuals. Additionally, it applies to any person or business that maintains computerized data on behalf of an information broker or data collector that includes personal information of individuals that is not owned.

Who must be notified?

Notification of the breach in the security of the data must be provided to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Entities that maintain computerized data on behalf of an information broker or data collector must notify the information broker or data collector of any breach within 24 hours following discovery if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

In the event that an information broker or data collector discovers circumstances requiring notification of more than 10,000 Georgia residents at one time, the information broker or data collector must also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nation-wide basis, as defined by 15 U.S.C. § 1681a, of the timing, distribution, and content of the notices.

When must they be notified?

Notice must be provided in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.

What must be included in the notification?

The content of the notification is not explicitly addressed in the statute.

How must they be notified?

Notice may be written, provided via telephone, or electronic. If electronic, the notice provided must remain consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001. Substitute notice may be provided if the information broker or data collector demonstrates that the cost of providing notice to affected individuals would exceed $50,000, the affected class of individuals to be notified exceeds 100,000, or that the information broker or data collector does not have sufficient contact information to provide written or electronic notice to such individuals.

Do any exceptions or exemptions apply?

Notification may be delayed if a law enforcement agency determines that the notification will compromise a criminal investigation.

What are the legal consequences for violating the law?

This statute does not address the legal consequences for violating these provisions.

HAWAII

H.R.S. § 487N-1 *et seq*.

What is a data breach?

"Security breach" means an incident of unauthorized access to and acquisition of unencrypted or unredacted records or data containing personal information where illegal use of the personal information has occurred, or is reasonably likely to occur and that creates a risk of harm to a person. Any incident of unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential process or key constitutes a security breach.

Who does this law apply to?

Any business that owns or licenses personal information of residents of Hawaii, any business that conducts business in Hawaii that owns or licenses personal information in any form (whether computerized, paper, or otherwise), or any government agency that collects personal

information for specific government purposes is subject to these provisions. In addition, any business located in Hawaii or any business that conducts business in Hawaii that maintains or possesses records or data containing personal information of residents of Hawaii that the business does not own or license, or any government agency that maintains or possesses records or data containing personal information of residents of Hawaii, is subject to these provisions.

Who must be notified?

Notice that there has been a security breach following discovery or notification of the breach must be provided to any affected person. In the event a business provides notice to more than one thousand persons at one time pursuant to this section, the business must notify the State of Hawaii's office of consumer protection and all consumer reporting agencies in writing, and without unreasonable delay, pursuant to 15 U.S.C. § 1681a(p).

When must they be notified?

The disclosure notification must be made without unreasonable delay, consistent with the legitimate needs of law enforcement, and consistent with any measures necessary to determine sufficient contact information, determine the scope of the breach, and restore the reasonable integrity, security, and confidentiality of the data system.

What must be included in the notification?

The notice shall include a description of the following:

(1) The incident in general terms;

(2) The type of personal information that was subject to the unauthorized access and acquisition;

(3) The general acts of the business or government agency to protect the personal information from further unauthorized access;

(4) A telephone number that the person may call for further information and assistance, if one exists; and

(5) Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports.

How must they be notified?

Notice to the affected persons may be provided by written notice to the last available address that the business or government agency has on record, electronic mail notice that is consistent with the requirements set forth in 15 U.S.C. § 7001 for those persons that an entity has a valid electronic mail address and who have agreed to receive communications electronically, or by telephone notice, provided that contact is made directly to the affected persons. Substitute notice is available if the entity demonstrates that providing notice would exceed $100,000, the affected class of persons to be notified exceeds 200,000, the entity does not have sufficient contact information or consent to satisfy the required notice, or the entity is unable to identify particular affected persons.

Do any exceptions or exemptions apply?

The notice required by this section may be delayed if a law enforcement agency informs the business or government agency that notification may impede a criminal investigation or jeopardize national security and requests a delay.

In addition, certain financial institutes are deemed in compliance with these statutes if subject to the federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice published in the Federal Register. Further, any health plan or healthcare provider that is subject to and in compliance with the standards for privacy or individually identifiable health information and the security standards for the protection of electronic health information are deemed in compliance with these provisions.

What are the legal consequences for violating the law?

The statute does not address the legal consequences for violating these statutes.

IDAHO

IDAHO CODE § 28-51-104 *et seq*.

What is a data breach?

"Breach of the security of the system" means the illegal acquisition of unencrypted computerized data that materially compromises the security, confidentiality, or integrity of personal information for one or more persons maintained by an agency, individual, or a commercial entity.

Who does this law apply to?

This law applies to any city, county or state agency, individual or a commercial entity that conducts business in Idaho and that owns or licenses computerized data that includes personal information about a resident of Idaho.

Who must be notified?

Notice must be provided to affected Idaho residents. When an agency becomes aware of a breach of the security of the system, it must also notify the office of the Idaho attorney general within 24 hours of discovery. Upon discovery of breach, a state agency must also report the security breach to the office of the chief information officer within the department of administration, pursuant to the Idaho technology authority policies.

When must they be notified?

When an entity becomes aware of a breach of the security of the system, it must conduct a reasonable and prompt investigation in good faith to determine the likelihood that personal information has been or will be misused. If the investigation determines that the misuse of information about an Idaho resident has occurred or is reasonably likely to occur, the agency, individual, or the commercial entity must provide notice as soon as possible.

What must be included in the notification?

The content of the notification is not explicitly addressed in the statute.

How must they be notified?

Notice may be provided by: written notice to the most recent address that the entity has in its records, telephonic notice, or electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001. Substitute notice is available if the entity required to provide notice demonstrates that the cost of providing

notice would exceed $25,000, or that the number of Idaho residents to be notified exceeds 50,000, or that the agency, individual, or the commercial entity does not have sufficient contact information to provide notice.

Do any exceptions or exemptions apply?

Notice required by this section may be delayed if a law enforcement agency advises the agency, individual or commercial entity that the notice will impede a criminal investigation.

An agency, individual or a commercial entity that maintains its own notice procedures that are otherwise consistent with the timing requirements of Idaho Code § 28-51-105, is deemed to be in compliance with the notice requirements if the entity notifies affected Idaho residents in accordance with its policies in the event of a breach of security of the system.

An entity that is regulated by state or federal law and that maintains procedures for a breach of the security of the system pursuant to the laws, rules, regulations, guidances, or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance with these provisions if the individual or the commercial entity complies with the maintained procedures when a breach of the security of the system occurs.

What are the legal consequences for violating the law?

If an entity's primary regulator has reason to believe that an agency, individual, or commercial entity subject to that primary regulator's jurisdiction pursuant to the Idaho Code, has violated the provisions of these statutes, the primary regulator may bring a civil action to enforce compliance with that section and enjoin that agency, individual, or commercial entity from further violations. Any entity that intentionally fails to give notice in accordance with the statute will be subject to a fine of not more than $25,000 per breach of the security system.

Any governmental employee who intentionally discloses personal information not subject to disclosure otherwise allowed by law is guilty of a misdemeanor and, upon conviction thereof, shall be punished by a fine of not more than two thousand dollars ($2,000), or by imprisonment in the county jail for a period of not more than one year, or both.

ILLINOIS

815 ILCS § 530/5, 530/10, 530/15, 530/20, 530/25

What is a data breach?

"Breach of the security of the system data" or "breach" is an unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the data collector. "Breach of the security of the system data" does not include the good faith acquisition of personal information by an employee or agent of the data collector for a legitimate purpose of the data collector, provided that the personal information is not used for a purpose unrelated to the data collector's business or subject to further unauthorized disclosure.

Who does this law apply to?

This law applies to any data collector that owns or licenses personal information concerning an Illinois resident. A data collector may include, but is not limited to, government agencies, public and private universities, privately and publicly held corporations, financial

institutions, retail operators, and any other entity that for any purpose, handles, collects, disseminates, or otherwise deals with nonpublic personal information.

In addition, any data collector that maintains or stores, but does not own or license, computerized data that includes personal information is subject to notification requirements if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Who must be notified?

Any entity to which the statute applies must notify any affected Illinois resident at no charge when there has been a breach following discovery or notification of the breach.

Data collectors that maintain or store, but do not own or license, computerized data that includes personal information must notify the owner or licensee of the information of any breach of the security of the data.

If a state agency is required to notify more than 1,000 persons of a breach of security, the state agency must also notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by 15 U.S.C. § 1681a(p).

When must they be notified?

The disclosure notification must be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.

What must be included in the notification?

The disclosure notification to an Illinois resident shall include, but need not be limited to, (i) the toll-free numbers and addresses for consumer reporting agencies, (ii) the toll-free number, address, and website address for the Federal Trade Commission, and (iii) a statement that the individual can obtain information from these sources about fraud alerts and security freezes. The notification shall not, however, include information concerning the number of Illinois residents affected by the breach.

How must they be notified?

Notice to consumers may be provided through written or electronic notice if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001. Substitute notice is available if the data collector demonstrates that the cost of providing notice 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.

Do any exceptions or exemptions apply?

Notification to an Illinois resident may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation. However, the state agency must notify the Illinois resident as soon as notification would no longer interfere with the investigation.

If an entity maintains its own notification procedures policy for the treatment of personal information and is consistent with the timing requirements of Illinois law, it will be deemed in compliance with the notification requirements of these provisions if the entity notifies subject persons in accordance with its policies in the event of a breach.

What are the legal consequences for violating the law?

A violation of this Act constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act.

INDIANA

IND. CODE ANN. § 24-4.9-1 *et seq.*; IND. CODE ANN. § 4-1-11 *et seq*.

What is a data breach?

"Breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person, or state or local agency. The term includes the unauthorized acquisition of computerized data that have been transferred to another medium, including paper, microfilm, or a similar medium, even if the transferred data are no longer in a computerized format.

Who does this law apply to?

This law applies to data base owners. A data base owner is any individual, a corporation, a business trust, an estate, a trust, a partnership, an association, a nonprofit corporation or organization, a cooperative, or any other legal entity that owns or licenses computerized data that includes personal information. Indiana law also provides that any state agency that owns or licenses computerized data that includes personal information is subject to data breach notification requirements.

Who must be notified?

Notification of the breach must be provided to any Indiana resident whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. In addition, an entity that maintains computerized data but that is not a data base owner shall notify the data base owner if the person discovers that personal information was or may have been acquired by an unauthorized person. Further, the attorney general must be notified regarding the breach. Moreover, if an entity is required to make a disclosure to more than 1,000 consumers, it must also provide notification of the breach to all nationwide consumer reporting agencies.

When must they be notified?

Notice must be provided within the most expedient time possible and without unreasonable delay. A delay is reasonable if the delay is necessary to restore the integrity of the computer system, necessary to discover the scope of the breach, or in response to a request from the attorney general or a law enforcement agency to delay disclosure.

What must be included in the notification?

The content of the notification is not explicitly addressed in the statute.

How must they be notified?

Notice may be provided by mail, telephone, or by email, if the entity has the email address of the affected Indiana resident. If an entity demonstrates that the cost of notification

would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000, substitute notice is available.

Do any exceptions or exemptions apply?

A delay in notification is permissible if requested by the attorney general or law enforcement agency because disclosure would impede a law enforcement investigation or jeopardize national security.

Entities subject to and in compliance with certain federal data security laws and regulations specified in the present statute are deemed in compliance with these statutes. In addition, if an entity maintains its own notification procedures and information privacy policies, it is not required to make a separate disclosure if the procedures are in compliance with the requirements set forth in the Indiana Code.

What are the legal consequences for violating the law?

A person that knowingly or intentionally fails to comply with any provision of this section commits a deceptive act that is actionable only by the attorney general. The attorney general may bring an action to obtain any or all of the following: (1) an injunction to enjoin future violations of the statute (2) a civil penalty of not more than one hundred fifty thousand dollars ($150,000) per deceptive act; (3) the attorney general's reasonable costs in: (a) the investigation of the deceptive act; and (b) maintaining the action; (4) reasonable attorney's fees, and (5) costs of the action.

IOWA

IOWA CODE ANN. § 715C.1-2

What is a data breach?

"Breach of security" means unauthorized acquisition of personal information maintained in computerized form by a person that compromises the security, confidentiality, or integrity of the personal information. A breach of security also means the unauthorized acquisition of personal information maintained by a person in any medium, including on paper, that was transferred by the person to that medium from computerized form and that compromises the security, confidentiality, or integrity of the personal information.

Who does this law apply to?

This law applies to any individual, corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture, government, governmental subdivision, agency, or instrumentality, public corporation, or any other legal or commercial entity that owns or licenses computerized data that includes an Iowa resident's personal information that is used in the course of the person's business, vocation, occupation, or volunteer activities. In addition, any entity that maintains or otherwise possesses personal information on behalf of another entity must comply with the notification requirements set forth under Iowa law.

Who must be notified?

Notice must be provided to any Iowa resident whose personal information was included in the information that was breached. If an entity subject to these provisions must provide notification to more than 500 Iowa residents, the entity must provide written notice of the breach

of security, or receipt of notification, to the director of the consumer protection division of the Officer of the Attorney General within five business days after giving notice of the breach of security to any affected Iowa resident.

When must they be notified?

Notice must be provided in the most expeditious manner possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to sufficiently determine contact information for the affected consumers, determine the scope of the breach, and restore the reasonable integrity, security, and confidentiality of the data.

What must be included in the notification?

The content of the notification is not explicitly addressed in the statute.

How must they be notified?

Written notice may be sent to the last available address the entity has in its records, or notice may be electronic if the entity's customary method of communication with consumers is electronic or is consistent with chapter 554D of 15 U.S.C. § 7001. Substitute notice is available if the entity demonstrates that the cost of providing notice would exceed $250,000, that the affected class of consumers to be notified exceeds 350,000 persons, or if the entity does not have sufficient contact information to provide notice.

Do any exceptions or exemptions apply?

The consumer notification requirements of this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. Notification requirements will not apply to an entity that complies with notification requirements or procedures that provide greater protection to personal information pursuant to the entity's primary or federal regulator, state or federal law or is in compliance with the regulations promulgated pursuant to 15 U.S.C. § 6801 – 6809.

What are the legal consequences for violating the law?

A violation of Iowa's data notification statute constitutes consumer fraud pursuant to IOWA CODE ANN. § 714.16. In addition to the remedies provided pursuant to § 714.16 subsection 7, the attorney general may seek damages against a party in violation of the notification requirements on behalf of those injured by the violation.

KANSAS

KAN. STAT. ANN. § 50-7a01 *et. seq*.

What is a data breach?

"Security breach" means the unauthorized access and acquisition of unencrypted or unredacted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an individual or a commercial entity and that causes, or such individual or entity reasonably believes has caused or will cause, identity theft to any consumer.

Who does this law apply to?

This law applies to any individual, partnership, corporation, trust, estate, cooperative, association, government, or governmental subdivision or agency or other entity ("entity") that conducts business in Kansas and that owns or licenses computerized data that includes personal information. An individual or a commercial entity that maintains computerized data that includes personal information that the individual or the commercial entity does not own or license must also provide notice in the event of a security breach, if the personal information was, or is reasonably believed to have been, accessed and acquired by an unauthorized person.

Who must be notified?

Notice must be provided to the affected Kansas resident. If more than 1,000 consumers must be notified at one time, an entity must also notify all consumer reporting agencies nationwide, pursuant to 15 U.S.C. § 1681a(p).

When must they be notified?

Notice must be provided in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.

What must be included in the notification?

The content of the notification is not explicitly addressed in the statute.

How must they be notified?

Notice may be written or electronic, if the electronic notice is consistent with 15 U.S.C. § 7001. Substitute notice is available if the entity required to provide notice demonstrates that the cost of providing notice will exceed $100,000, or that the affected class of consumers will exceed 5,000, or that the entity does not have sufficient contact information to provide notice.

Do any exceptions or exemptions apply?

Notice may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation. In addition, an entity that maintains its own notification procedures that are consistent with the timing requirements under Kansas law is deemed to be in compliance with the notice requirements if the entity notifies affected consumers in accordance with its policies. Further, an entity that is regulated by state or federal law and that maintains procedures for a breach of the security of the system pursuant to the laws, rules, regulations, guidances or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance with the requirements set forth under Kansas law.

What are the legal consequences for violating the law?

The attorney general may bring an action to address an entity's violations to enforce compliance and enjoin future violations. If an insurance company violates these provisions, the insurance commission has sole authority to enforce the notification requirements.

KENTUCKY
2014 KY H.B. 5, 2014 KY H.B. 232

What is a data breach?

"Breach of the security of the system" means the unauthorized acquisition of unencrypted and unredacted computerized data that compromises the security, confidentiality, or integrity of personally identifiable information maintained by the information holder as part of a database regarding multiple individuals that actually causes, or leads the information holder to reasonably believe he has caused or will cause, identity theft or fraud against any Kentucky resident.

Who does this law apply to?

This law applies to any person or business entity ("information holder") that conducts business in Kentucky. In addition, an agency or nonaffiliated third party that maintains or otherwise possesses personal information, regardless of the form in which the personal information is maintained, must implement, maintain, and update security procedures and practices, including taking any appropriate corrective action, to protect and safeguard against security breaches.

Who must be notified?

Any information holder must disclose any breach of the security of the system, following discovery or notification of the breach in the security of the data, to any Kentucky resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. If notification is required of more than 1,000 persons at a time, the information holder must also notify all consumer reporting agencies and credit bureaus pursuant to 15 U.S.C. § 1681a.

In addition, any agency that collects, maintains, or stores personal information that determines or is notified of a security breach relating to personal information collected, maintained, or stored by the agency or by a nonaffiliated third-party on behalf of the agency, must notify the Commissioner of the Kentucky State Police, the Auditor of Public Accounts, and the Attorney General.

When must they be notified?

The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. Any agency or nonaffiliated third-party on behalf of the agency must provide notification within 72 hours of determination or notification of breach.

What must be included in the notification?

The content of the notification is not explicitly addressed in the statute.

How must they be notified?

Notification may be provided through written notice, or electronic notice, if the electronic notice is consistent with the requirements set forth in 15 U.S.C. § 7001. Substitute notice is available if the information holder demonstrates that the cost of providing notice would exceed

$250,000, or that the affected class of subject persons to be notified exceeds 500,000, or the information holder does not have sufficient contact information.

Do any exceptions or exemptions apply?

Notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. In addition, an information holder that maintains its own notification procedures that are consistent with the timing requirements of Kentucky's notification provisions is deemed in compliance with the Kentucky notification statutes.

Moreover, the requirements for nonaffiliated third parties does not apply to any entity subject to the provisions of Title V of the Gramm-Leach-Bliley Act, the federal Health Insurance Portability and Accountability Act, any Kentucky agency, or any Kentucky local governments or political subdivisions.

What are the legal consequences for violating the law?

The Kentucky statutes do not address the legal consequences for violating the notification requirements.

LOUISIANA

LA. REV. STAT. § 51:3071 *et seq*.

What is a data breach?

"Breach of the security of the system" means the compromise of the security, confidentiality, or integrity of computerized data that results in, or there is a reasonable basis to conclude has resulted in, the unauthorized acquisition of and access to personal information maintained by an agency or person.

Who does this law apply to?

This law applies to any individual, corporation, partnership, sole proprietorship, joint stock company, joint venture, or any other legal entity that conducts business in Louisiana, that owns, does not own, or licenses computerized data that includes personal information. This law also applies to any agency that owns, does not own, or licenses computerized data that includes personal information.

Who must be notified?

Notification must be provided to any Louisiana resident whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

When must they be notified?

Notification must be provided as expediently as possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or any measures necessary to determine the scope of the breach, prevent further disclosures, and restore the reasonable integrity of the data system.

What must be included in the notification?

The content of the notification is not explicitly addressed in the statute.

How must they be notified?

Notification may be provided through written notice, or electronic notice, if the electronic notice is consistent with the requirements set forth under 15 U.S.C. § 7001. Substitute notification is available if an agency or entity demonstrates that the cost of providing notification would exceed $250,000, the affected class of persons to be notified exceeds 500,000, or the agency or person does not have sufficient contact information.

Do any exceptions or exemptions apply?

Notification may be delayed if a law enforcement agency determines that notification would impede a criminal investigation. In addition, an agency or person that maintains a notification procedure that is otherwise consistent with said timing requirements is deemed to be in compliance with the notification requirements under Louisiana law if the agency or person notifies subject persons in accordance with the policy and procedure in the event of a breach of security of the system.

Moreover, a financial institution that is subject to and in compliance with the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, and any revisions, additions, or substitutions relating to said interagency guidance, is deemed to be in compliance with Louisiana's notification requirements.

What are the legal consequences for violating the law?

A civil action may be instituted to recover actual damages resulting from the failure to disclose in a timely manner to a person that there has been a breach of the security system resulting in the disclosure of a person's personal information.

In addition, failure to provide timely notice may be punishable by a fine not to exceed $5,000 per violation.

MAINE

10 ME. REV. STAT. § 1346 *et seq*.

What is a data breach?

"Breach of the security of the system" or "security breach" means unauthorized acquisition, release or use of an individual's computerized data that includes personal information that compromises the security, confidentiality, or integrity of personal information of the individual maintained by a person.

Who does this law apply to?

This law applies to any individual, partnership, corporation, limited liability company, trust, estate, cooperative, association or other entity, including agencies of State Government, the University of Maine System, the Maine Community College System, Maine Maritime Academy and private colleges and universities, or any information broker, that maintains computerized data that includes personal information. In addition, this law also applies to any third-party entity that maintains, on behalf of a person, computerized data that includes personal information that the third-party entity does not own.

Who must be notified?

Notification of the security breach must be provided to any affected Maine resident if misuse of the personal information has occurred or if it is reasonably possible that misuse will occur. Additionally, when notice of a breach of the security of the system is required, the entity must notify the appropriate state regulators within the Department of Professional and Financial Regulation, or if the person is not regulated by the department, the Attorney General.

Moreover, if a breach requires notification to more than 1,000 persons at a single time, an entity must also notify, without unreasonable delay, consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, pursuant to 15 U.S.C. § 1681a(p).

When must they be notified?

Notice must be provided as expediently as possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or with measures necessary to determine the scope of the security breach and restore the reasonable integrity, security, and confidentiality of the data in the system.

What must be included in the notification?

The content of the notification is not explicitly addressed in the statute.

How must they be notified?

Notification may be provided through written notice, or electronic notice, if the electronic notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001. Substitute notice is available if the entity maintaining personal information demonstrates that the cost of providing notice would exceed $5,000, that the affected class of individuals to be notified exceeds 1,000, or that the person maintaining personal information does not have sufficient contact information to provide written or electronic notice to affected individuals.

Do any exceptions or exemptions apply?

Notification may not be delayed for longer than seven business days after a law enforcement agency determines that the notification will not compromise a criminal investigation.

In addition, an entity that complies with the security breach notification requirements of rules, regulations, procedures, or guidelines established pursuant to federal law or Maine law is deemed to be in compliance as long as the law, rules, regulations or guidelines provide for notification procedures at least as protective as the notification requirements.

What are the legal consequences for violating the law?

A person that violates this law commits a civil violation and is subject to civil penalties in the amount of $500 per violation, up to a maximum of $2,500 each day the person is in violation; equitable relief; or enjoinment from further violations of this chapter.

MARYLAND

MD. CODE COM. LAW § 14-3501 *et seq*.

What is a data breach?

"Breach of the security of a system" means the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of the personal information maintained by a business.

Who does this law apply to?

This law applies to any sole proprietorship, partnership, corporation, association, or any other business entity, whether or not organized to operate a profit, including a financial institution, organized, chartered, licensed, or otherwise authorized under Maryland law, any other state, the United States, or any other country that owns or licenses computerized data that includes personal information of Maryland residents.

Who must be notified?

A business must first provide notice of a breach of the security of a system to the Office of the Attorney General. Then, notice must be provided to any Maryland resident whose personal information has been misused or is reasonably likely to be misused as a result of a breach of the security of a system. In addition, if an entity must notify 1,000 or more individuals, the entity must also notify, without unreasonable delay, each consumer reporting agency on a nationwide basis pursuant to 15 U.S.C. § 1681a(p).

When must they be notified?

A business that owns or licenses computerized data that includes personal information of Maryland residents, when it discovers or is notified of a breach of the security of a system, must conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information of the individual has been or will be misused as a result of the breach. If, after the investigation is concluded, the business determines that misuse of the individual's personal information has occurred or is reasonably likely to occur as a result of a breach of the security of a system, the business must notify the individual of the breach.

What must be included in the notification?

The notification shall include:

> (1) To the extent possible, a description of the categories of information that were, or are reasonably believed to have been, acquired by an unauthorized person, including which of the elements of personal information were, or are reasonably believed to have been, acquired;
>
> (2) Contact information for the business making the notification, including the business' address, telephone number, and toll-free telephone number if one is maintained;
>
> (3) The toll-free telephone numbers and addresses for the major consumer reporting agencies; and
>
> (4) (i) The toll-free telephone numbers, addresses, and Web site addresses for: 1. The Federal Trade Commission; and 2. The Office of the Attorney General; and

(ii) A statement that an individual can obtain information from these sources about steps the individual can take to avoid identity theft.

How must they be notified?

Notice may be provided by written notice; electronic mail, if the individual has expressly consented to receive electronic notice or the business conducts its business primarily through Internet account transactions or the Internet; or by telephonic notice. Substitute notice may be available if the business demonstrates that the cost of providing notice would exceed $100,000, that the affected class of individuals to be notified exceeds 175,000, or the business does not have sufficient contact information to provide notice.

Do any exceptions or exemptions apply?

Notice may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation or jeopardize homeland or national security.

In addition, an entity that complies with the requirements for notification procedures under the rules, regulations, procedures, or guidelines established by a primary or functional federal or state regulator of the business will be deemed in compliance with the statute. Further, an entity or the affiliate of an entity that is subject to and in compliance with the Gramm-Leach-Bliley Act pursuant to 15 U.S.C. § 6801, § 216 of the federal Fair and Accurate Credit Transactions Act, 15 U.S.C. § 1681w, the federal Interagency Guideline Establishing Information Security Standards, and the federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, and any revisions, additions, or substitutions, will be deemed in compliance with the statute.

What are the legal consequences for violating the law?

Consumers may file actions under Title 13 of the Maryland Code, the Unfair and Deceptive Trade Practices Act, in the event of violation.

MASSACHUSETTS

MASS. GEN. LAWS 93H § 1 *et seq.*

What is a data breach?

"Breach of security" means the unauthorized acquisition/use of unencrypted data or encrypted electronic data (and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information) maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the commonwealth.

A good faith but unauthorized acquisition of personal information by a person or agency, or employee or agent thereof, for the lawful purposes of such person or agency, is not a breach of security unless the personal information is used in an unauthorized manner or subject to further unauthorized disclosure.

Who does this law apply to?

A person or agency that maintains, stores, owns, or licenses data that includes personal information about a resident of the Commonwealth.

Who must be notified?

When a person/agency does not own and/or license personal information, the owner/licensor of the personal information must be notified as well as the resident that may have been affected by the breach of security or unauthorized acquisition or use. When a person/agency owns and/or licenses personal information, the resident, the attorney general, and the director of consumer affairs and business regulation must be notified.

When must they be notified?

As soon as practicable without unreasonable delay after the person or agency knows or has reason to know of a security breach, or knows or has reason to know that the personal information of a resident was acquired and/or used by an unauthorized person or used for an unauthorized purpose.

How must they be notified?

Written notice or electronic substitute notice, if the person or agency required to provide notice demonstrates that the cost of providing written notice will exceed $250,000, or that the affected class of Massachusetts residents to be notified exceeds 500,000 residents, or that the person or agency does not have sufficient contact information to provide notice.

"Substitute notice" shall consist of all of the following: electronic mail notice, if the person or agency has electronic mail addresses for the members of the affected class of Massachusetts residents; clear and conspicuous posting of the notice on the home page of the person or agency if the person or agency maintains a website; and publication in or broadcast through media or medium that provides notice throughout the Commonwealth.

What must be included in the notification?

For all breaches, a resident whose information was breached must be notified of information regarding: the consumer's right to obtain a police report, how a consumer requests a security freeze and the necessary information to be provided when requesting the security freeze, and any fees required to be paid to any of the consumer reporting agencies. When a person/agency is not the owner/licensor of personal information, in addition to notifying the resident of the information discussed above, the owner/licensor of the information must be notified of: the date/approximate date of the unauthorized acquisition or use, the nature of the unauthorized acquisition or use, and any steps the person/agency has taken to remedy the breach. When a person/agency is the owner/licensor of personal information, in addition to notifying the resident, notice provided to the attorney general and said director, and consumer reporting agencies or state agencies if any, shall include, but not be limited to, the nature of the breach of security or unauthorized acquisition or use, the number of residents of the Commonwealth affected by such incident at the time of notification, and any steps the person or agency has taken or plans to take relating to the incident.

Do any exceptions or exemptions apply?

Notice may be delayed if a law enforcement agency determines that notice may impede a criminal investigation and has notified the attorney general, in writing, thereof and informs the person or agency of such determination.

What are the legal consequences for violating the law?

The attorney general may bring an action pursuant to section 4 of chapter 93A against a

person or otherwise to remedy violations of this chapter and for other relief that may be appropriate.

MICHIGAN

MICH. COMP. LAWS § 445.63, 72 et seq.

What is a data breach?

"Breach of the security of a database" or "security breach" means the unauthorized access and acquisition of data that compromises the security or confidentiality of personal information maintained by a person or agency as part of a database of personal information regarding multiple individuals. A breach does not include unauthorized access to data by an employee or other individual if the employee or other individual acted in good faith in accessing the data, the access was related to the activities of the agency or person, or the employee or other individual did not misuse any personal information or disclose any personal information to an unauthorized person.

Who does this law apply to?

Any department, board, commission, office, agency, authority, individual, partnership, corporation, or other entity maintaining the personal information of Michigan residents, whether or not organized or licensed under the laws of Michigan.

Who must be notified?

Unless the person or agency determines that the security breach has not or is not likely to cause substantial loss or injury to, or result in identity theft with respect to, one or more residents, a person or agency that owns or licenses data that is included in a database that discovers a security breach, or receives notice of a security breach shall provide notice of the security breach to each resident who meets one or more of the following: (a) that resident's unencrypted and unredacted personal information was accessed and acquired by an unauthorized person; or (b) that resident's personal information was accessed and acquired in encrypted form by a person with unauthorized access to the encryption key.

A person or agency that maintains a database that includes data that the person or agency does not own or license that discovers a breach of the security of the database shall provide notice to the owner or licensor of the information of the security breach.

When must they be notified?

A person or agency shall provide notice without unreasonable delay following the discovery of the breach.

What must be included in the notification?

A description of the security breach in general terms must be included in the notification as well as a description of the type of personal information that was accessed without authorization (if applicable), a general description of the agency/person's subsequent steps to protect the data from further security breaches, a telephone number of where notice recipient may obtain assistance or additional information, and a reminder to notice recipients of the need to remain vigilant for incidents of fraud and identity theft.

How must they be notified?

Notice may be by written and sent to the recipient's address or by electronic notice when the recipient has expressly consented to receive electronic notice, the person or agency has an existing business relationship with the recipient that includes periodic electronic mail communications and based on those communications the person or agency reasonably believes that it has the recipient's current electronic mail address, or the person or agency conducts its business primarily through internet account transactions or on the internet. Notice by telephone may be given when the notice is not given in whole or in part by use of a recorded message and the recipient has expressly consented to receive notice by telephone, or if the recipient has not expressly consented to receive notice by telephone, the person or agency also provides notice through written or electronic notice if the notice by telephone does not result in a live conversation between the individual representing the person or agency and the recipient within three business days after the initial attempt to provide telephonic notice.

Substitute notice is allowed if the person or agency demonstrates that the cost of providing notice will exceed $250,000.00 or that the person or agency has to provide notice to more than 500,000 residents of this state. A person or agency provides substitute notice under this subdivision by doing all of the following: if the person or agency has electronic mail addresses for any of the residents of this state who are entitled to receive the notice, providing electronic notice to those residents; if the person or agency maintains a website, conspicuously posting the notice on that website; notifying major statewide media, including a telephone number or a website address that a person may use to obtain additional assistance and information.

Do any exceptions or exemptions apply?

Notification is not required if the entity determines that the security breach has not or is not likely to cause substantial loss or injury to, or result in identity theft with respect to, one or more residents of Michigan.

Notification can be delayed in order for the person or agency to determine the scope of the security breach and the measures necessary to restore the reasonable integrity of the database; or if a law enforcement agency determines and advises the agency/person that providing notice will impede a criminal or civil investigation or jeopardize homeland or national security.

What are the legal consequences for violating the law?

A person that knowingly fails to provide any notice of a security breach required under this section may be ordered to pay a civil fine of not more than $250 for each failure to provide notice. The attorney general or a prosecuting attorney may bring an action to recover a civil fine under this section.

MINNESOTA

MINN. STAT. §§ 325E.61

What is a data breach?

A "Security Breach" is an unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. A breach does not include a good faith acquisition by an employee or agent of the person or business for the purposes of the person or business. This statute is not applicable if the compromised data is encrypted.

Who does this law apply to?

This law applies to any person or entity doing business in Minnesota that collects and stores personal information of customers.

Who must be notified?

Compromised persons and entities must be notified. If more than 500 persons at one time require notification, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis must be notified within 48 hours.

When must they be notified?

Notification must occur at the most expedient time possible without undue delay.

What must be included in the notification?

Notification should include any breach of the security of the system following discovery or notification of the breach in the security of the data.

How must they be notified?

Written notice to the most recent available address of the person or business should be provided or electronic notice if the person's primary method of communication with the individual is by electronic means, or if the notice is consistent with the provisions regarding electronic records and signatures in U.S. Code title 15 § 7001.

Substitute notice is allowed if the cost of providing notice would exceed $250,000, or the affected class of persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information.

Do any exceptions or exemptions apply?

Notice may be delayed to a date certain if a law enforcement agency determines that notification will impede a criminal investigation.

What are the legal consequences for violating the law?

The attorney general shall enforce violations of this statute.

MISSISSIPPI

MISS. CODE § 75-24-29

What is a data breach?

"Breach of security" means unauthorized acquisition of electronic files, media, databases or computerized data containing personal information of any resident of this state when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable.

Who does this law apply to?

The law applies to any persons conducting business in Mississippi that maintains, owns, or licenses computerized data that includes personal information.

Who must be notified?

A person who conducts business in this state shall disclose any breach of security to all affected individuals.

When must they be notified?

Notification should occur without undue delay.

What must be included in the notification?

Affected individuals must be notified of the information of any breach of the security of the data.

How must they be notified?

Written notice, telephonic notice, or electronic notice is sufficient if the entity's primary method of communication with the affected individual is electronic, or if the notice is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001.

Substitute notice is permitted if the cost of notification would exceed $5,000 or if persons to be notified exceed 5,000.

Do any exceptions or exemptions apply?

Notice is not required if, after appropriate investigation, the person reasonably determines that the breach will not likely result in harm to those affected individuals. Notice may be delayed if the law enforcement agency determines such notice will impede an ongoing criminal investigation or compromise national security.

Any person who conducts business in this state that maintains its own security breach procedures as part of an information security policy for the treatment of personal information, and otherwise complies with the timing requirements of this section, shall be deemed to be in compliance with the security breach notification requirements if the person notifies affected individuals in accordance with the person's policies in the event of a breach of security.

Any person that maintains such a security breach procedure pursuant to the rules, regulations, procedures, or guidelines established by the primary or federal functional regulator, as defined in 15 U.S.C. § 6809(2), shall be deemed to be in compliance with the security breach notification requirements, provided the person notifies affected individuals in accordance with the policies or the rules, regulations, procedures, or guidelines established by the primary or federal functional regulator in the event of a breach of security of the system.

What are the legal consequences for violating the law?

Failure to provide notice shall constitute an unfair trade practice and shall be enforced by the attorney general. There is no private right of action under this section.

MISSOURI

MO. REV. STAT. § 407.1500

What is a data breach?

A data breach is the unauthorized access to and unauthorized acquisition of personal information maintained in computerized form by a person that compromises the security, confidentiality, or integrity of the personal information.

The good faith acquisition of personal information by a person or that person's employee or agent for a legitimate purpose of that person is not a breach of security, provided that the

personal information is not used in violation of applicable law or in a manner that harms or poses an actual threat to the security, confidentiality, or integrity of the personal information.

Who does this law apply to?

Any individual, corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture, government, governmental subdivision, governmental agency, governmental instrumentality, public corporation, or any other legal or commercial entity that owns or licenses personal information of residents of Missouri or that conducts business in Missouri that owns or licenses personal information in any form of a resident of Missouri.

Who must be notified?

Affected individuals must be notified. When persons notified exceeds 1,000, the attorney general and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis must be notified of the timing, distribution, and content of the notice.

When must they be notified?

Affected individuals must be notified without unreasonable delay, consistent with the needs of law enforcement.

What must be included in the notification?

A description of the data breach incident in general terms must be included as well as the type of personal information that was compromised, a telephone number that the affected individual my 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.

How must they be notified?

Written notice, telephonic notice, or electronic notice is permitted for consumers with valid e-mail addresses who have agreed to receive communications electronically so long as notice provided is consistent with 15 U.S.C. § 7001.

Substitute notice is allowed if the cost would exceed $100,000, if the number of affected persons to be notified would exceed 150,000, or if the notifying entity does not have sufficient contact information or consent to notify the affected individual(s).

Do any exceptions or exemptions apply?

A person/entity that maintains its own notice procedures as part of an information security policy for the treatment of personal information, and whose procedures are otherwise consistent with the timing requirements of this section, is deemed to be in compliance with the notice requirements of this section if the person notifies affected consumers in accordance with its policies in the event of a breach of security of the system.

A person/entity that is regulated by state or federal law and that maintains procedures for a breach of the security of the system pursuant to the laws, rules, regulations, guidances, or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance with this section if the person notifies affected consumers in accordance with the maintained procedures when a breach occurs.

A financial institution that is subject to and in compliance with the Federal Interagency Guidance Response Programs for Unauthorized Access to Customer Information and Customer Notice, issued on March 29, 2005, by the board of governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision, and any revisions, additions, or substitutions relating to said interagency guidance; or subject to and in compliance with the National Credit Union Administration regulations in 12 CFR Part 748; or subject to and in compliance with the provisions of Title V of the Gramm-Leach-Bliley Financial Modernization Act of 1999, 15 U.S.C. §§ 6801 to 6809 shall be deemed to be in compliance with this section.

What are the legal consequences for violating the law?

The attorney general has the exclusive authority to bring an action to obtain actual damages and may seek a civil penalty not exceeding $150,000 per security breach or series of similar breaches.

MONTANA

MONT. CODE § 2-6-501 – 504 *et seq.*

What is a data breach?

"Breach of the security of a data system" or "breach" means the unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the person or business and causes or is reasonably believed to cause loss or injury to a Montana resident.

Who does this law apply to?

Any person or business that conducts business in Montana and that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the data system following discovery or notification of the breach to any resident of Montana whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person.

Who must be notified?

Any person whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person must be notified.

When must they be notified?

The notification must be made without unreasonable delay, consistent with the legitimate needs of law enforcement or with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system.

What must be included in the notification?

The content of the notification is not explicitly addressed in the statute.

How must they be notified?

A person may be notified by written notice, electronic notice (if consistent with 15 U.S.C. § 7001), telephonic notice, or substitute notice, if person/business demonstrates cost of notice will exceed $250,000 or the affected class of persons exceeds 500,000, or the person or business

does not have sufficient contact information.

Do any exceptions or exemptions apply?

A person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and that does not unreasonably delay notice is considered to be in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the data system.

Notice may be delayed if law enforcement agency determines providing notice would impede an ongoing criminal investigation.

What are the legal consequences for violating the law?

Legal consequences for violating this law are not addressed by the statute.

NEBRASKA

NEB. REV. STAT. §§ 87-801 – 807

What is a data breach?

Breach of the security of the system means the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an individual or a commercial entity.

Good faith acquisition of personal information by an employee or agent of an individual or a commercial entity for the purposes of the individual or the commercial entity is not a breach of the security of the system if the personal information is not used or subject to further unauthorized disclosure.

Acquisition of personal information pursuant to a search warrant, subpoena, or other court order or pursuant to a subpoena or order of a state agency is not a breach of the security of the system.

Who does this law apply to?

The law applies to any individual or commercial entity that maintains personal information. Commercial entities include: a corporation, business trust, estate, trust, partnership, limited partnership, limited liability partnership, limited liability company, association, organization, joint venture, government, governmental subdivision, agency, or instrumentality, or any other legal entity, whether for profit or not for profit.

Who must be notified?

If the investigation determines that the use of information about a Nebraska resident for an unauthorized purpose has occurred or is reasonably likely to occur, the individual or commercial entity shall give notice to the affected Nebraska resident.

When must they be notified?

Affected residents must be notified as soon as possible without unreasonable delay (consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system).

Notification is not required if after a good faith, reasonable and prompt investigation, the person/commercial entity determines that it is unlikely that personal information has been or will

be used for an unauthorized purpose.

What must be included in the notification?

An individual or a commercial entity that maintains computerized data that includes personal information that the individual or commercial entity does not own or license shall give notice to and cooperate with the owner or licensee of the information of any breach of the security of the system when it becomes aware of a breach if use of personal information about a Nebraska resident for an unauthorized purpose occurred or is reasonably likely to occur.

Cooperation includes, but is not limited to, sharing with the owner or licensee information relevant to the breach, not including information proprietary to the individual or commercial entity.

How must they be notified?

Written notice, telephonic notice, or electronic notice in compliance with 15 U.S.C. § 7001 is permitted. Substitute notice is allowed if the individual or commercial entity required to provide notice demonstrates that the cost of providing notice will exceed $75,000, that the affected class of Nebraska residents to be notified exceeds 100,000, or that the individual or commercial entity does not have sufficient contact information to provide notice.

Do any exceptions or exemptions apply?

An individual or a commercial entity that maintains its own notice procedures which are part of an information security policy for the treatment of personal information and which are otherwise consistent with the timing requirements of § 87-803, is deemed to be in compliance with the notice requirements of § 87-803 if the individual or the commercial entity notifies affected Nebraska residents in accordance with its notice procedures in the event of a breach of the security of the system.

An individual or a commercial entity that is regulated by state or federal law and that maintains procedures for a breach of the security of the system pursuant to the laws, rules, regulations, guidances, or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance with § 87-803 if the individual or commercial entity notifies affected Nebraska residents in accordance with the maintained procedures in the event of a breach of the security of the system.

What are the legal consequences for violating the law?

The attorney general may issue subpoenas and seek and recover direct economic damages for each affected Nebraska resident injured by a violation of the act.

NEVADA

NEV. REV. STAT. §§ 603A *et seq.*

What is a data breach?

"Breach of the security of the system data" means unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the data collector.

A breach does not include the good faith acquisition of personal information by an employee or agent of the data collector for a legitimate purpose of the data collector, so long as the personal information is not used for a purpose unrelated to the data collector or subject to

further unauthorized disclosure.

Who does this law apply to?

This law applies to any governmental agency, institution of higher education, corporation, financial institution or retail operator or any other type of business entity or association that, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates, or otherwise deals with nonpublic personal information.

Who must be notified?

Any data collector that owns or licenses computerized data which includes personal information shall disclose any breach of the security of the system data following discovery or notification of the breach to any resident of the state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Any data collector that maintains computerized data which includes personal information that the data collector does not own shall notify the owner or licensee of the information of any breach of the security of the system data immediately following discovery if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

If personal information of more than 1,000 persons is compromised, any consumer reporting agency as defined by 15 U.S.C. § 1681a(p) that compiles and maintains files on consumers on a nationwide basis must be notified of the time the notification is distributed and the content of the notification.

When must they be notified?

Notification must occur in the most expedient time possible without unreasonable delay.

What must be included in the notification?

The content of the notification is not explicitly addressed in the statute.

How must they be notified?

Written notification or electronic notification pursuant to 15 U.S.C. § 7001 may be given.

Substitute notification is allowed if the data collector demonstrates that 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.

Do any exceptions or exemptions apply?

A data collector that maintains its own notification policies and procedures as part of an information security policy for the treatment of personal information that is otherwise consistent with the timing requirements of this section shall be deemed to be in compliance with the notification requirements if the data collector notifies subject persons in accordance with its policies and procedures in the event of a breach of the security of the system data.

A data collector that is subject to and complies with the privacy and security provisions of the Gramm-Leach-Bliley Act,15 U.S.C. §§ 6801 *et seq*., shall be deemed to be in compliance with the notification requirements

Notification may be delayed due to determination of law enforcement agency that such notice would impede a criminal investigation.

What are the legal consequences for violating the law?

A data collector that provides the notification required pursuant to NRS 603A.220 may commence an action for damages against a person that unlawfully obtained or benefited from personal information obtained from records maintained by the data collector. A data collector that prevails in such an action may be awarded damages which may include, without limitation, the reasonable costs of notification, reasonable attorney's fees and costs and punitive damages when appropriate. The costs of notification include, without limitation, labor, materials, postage and any other costs reasonably related to providing the notification.

In addition to any other penalty provided by law for the breach of the security of the system data maintained by a data collector, the court may order a person who is convicted of unlawfully obtaining or benefiting from personal information obtained as a result of such breach to pay restitution to the data collector for the reasonable costs incurred by the data collector in providing the notification required pursuant to NRS 603A.220, including, without limitation, labor, materials, postage and any other costs reasonably related to providing such notification.

If the attorney general or a district attorney of any county has reason to believe that any person is violating, proposes to violate, or has violated the provisions of this chapter, the attorney general or district attorney may bring an action against that person to obtain a temporary or permanent injunction against the violation.

NEW HAMPSHIRE

N.H. REV. STAT. §§ 359-C:19-C:21

What is a data breach?

"Security breach" means unauthorized acquisition of computerized data that compromises the security or confidentiality of personal information maintained by a person doing business in this state.

Good faith acquisition of personal information by an employee or agent of a person for the purposes of the person's business shall not be considered a security breach, provided that the personal information is not used or subject to further unauthorized disclosure.

Who does this law apply to?

The law applies to any individual, corporation, trust, partnership, incorporated or unincorporated association, limited liability company, or other form of entity, or any agency, authority, board, court, department, division, commission, institution, bureau, or other state governmental entity, or any political subdivision of the state, doing business in this state who owns or licenses computerized data that includes personal information.

Who must be notified?

Any person doing business in this state who owns or licenses computerized data that includes personal information shall, when it becomes aware of a security breach, promptly determine the likelihood that the information has been or will be misused. If the determination is that misuse of the information has occurred or is reasonably likely to occur, or if a determination cannot be made, the person shall notify the affected individuals as soon as possible as required under this subdivision.

Any person engaged in trade or commerce that is subject to RSA 358-A:3 shall also notify the regulator which has primary regulatory authority over such trade or commerce.

All other persons shall notify the New Hampshire attorney general's office. The notice shall include the anticipated date of the notice to the individuals and the approximate number of individuals in this state who will be notified.

Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify and cooperate with the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was acquired by an unauthorized person.

When must they be notified?

Notification should occur as soon as possible after the entity has become aware of a security breach and determined that the breach has, or likely will, result in the misuse of privileged information.

What must be included in the notification?

The notification should include a description of the incident in general terms, the approximate date of the breach, the type of personal information obtained as a result of the security breach, and telephonic contact information of the business/entity whose database was breached.

How must they be notified?

Written notice or electronic notice is permitted if the agency's/business's primary means of communication with the affected individual is by electronic means.

Telephonic notice is permitted, provided that a log of each such notification is kept by the person or business who notifies affected persons.

Substitute notice is allowed if demonstrated that the cost of providing notice would exceed $5,000, that the affected class of subject individuals to be notified exceeds 1,000, or the person does not have sufficient contact information or consent to otherwise provide notice.

Do any exceptions or exemptions apply?

Notification may be delayed if law enforcement agency or national homeland security agency determines that the notification will impede a criminal investigation or otherwise jeopardize national security.

What are the legal consequences for violating the law?

Any person injured by any violation under this subdivision may bring an action for damages and for such equitable relief, including an injunction, as the court deems necessary and proper. If the court finds for the plaintiff, recovery shall be in the amount of actual damages. If the court finds that the act or practice was a willful or knowing violation of this chapter, it shall award as much as three times, but not less than two times, such amount. In addition, a prevailing plaintiff shall be awarded the costs of the suit and reasonable attorney's fees, as determined by the court. Any attempted waiver of the right to the damages set forth in this paragraph shall be void and unenforceable. Injunctive relief shall be available to private individuals under this chapter without bond, subject to the discretion of the court.

The New Hampshire attorney general's office shall enforce the provisions of this subdivision pursuant to RSA 358-A:4.

The burden shall be on the person responsible for the determination under RSA 359-C:20 to demonstrate compliance with this subdivision.

NEW JERSEY
N.J. STAT. § 56:8-163

What is a data breach?

"Breach of security" means unauthorized access to electronic files, media or data containing personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable.

Good faith acquisition of personal information by an employee or agent of the business for a legitimate business purpose is not a breach of security, provided that the personal information is not used for a purpose unrelated to the business or subject to further unauthorized disclosure.

Who does this law apply to?

This law applies to any business that conducts business in New Jersey, or any public entity that compiles or maintains computerized records that include personal information

Who must be notified?

Any business that conducts business in New Jersey, or any public entity that compiles or maintains computerized records that include personal information, shall disclose any breach of security of those computerized records following discovery or notification of the breach to any customer who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person.

Any business or public entity that compiles or maintains computerized records that include personal information on behalf of another business or public entity shall notify that business or public entity, who shall notify its New Jersey customers of any breach of security of the computerized records immediately following discovery, if the personal information was, or is reasonably believed to have been, accessed by an unauthorized person.

Any business or public entity required to disclose a breach of security of a customer's personal information shall, in advance of the disclosure to the customer, report the breach of security and any information pertaining to the breach to the Division of State Police in the Department of Law and Public Safety for investigation or handling, which may include dissemination or referral to other appropriate law enforcement entities.

If there are more than 1,000 affected persons, all consumer reporting agencies that compile or maintain files on consumers on a nationwide basis, as defined in subsection (p) of section 603 of the federal "Fair Credit Reporting Act" (15 U.S.C. §1681a), must be notified of the timing, distribution, and content of the notices.

When must they be notified?

Notice must be given without unreasonable delay.

What must be included in the notification?

The content of the notification is not explicitly addressed in the statute.

How must they be notified?

Written notice and electronic notice pursuant to 15 U.S.C. § 7001 are permitted.

Substitute notice is allowed if the cost of notice would exceed $250,000, the persons to be notified exceeds 500,000, or the business/public entity lacks sufficient contact information.

Do any exceptions or exemptions apply?

A business or public entity that maintains its own notification procedures as part of an information security policy for the treatment of personal information, and is otherwise consistent with the requirements of this section, shall be deemed to be in compliance with the notification requirements if the business or public entity notifies subject customers in accordance with its policies in the event of a breach of security of the system

Notification may be delayed if law enforcement agency determines notification will impede a criminal or civil investigation.

What are the legal consequences for violating the law?

The legal consequences of violating the law are not explicitly stated.

NEW YORK

N.Y. GEN. BUS. LAW § 899-aa, N.Y. State Tech. Law 208

What is a data breach?

"Breach of the security of the system" means unauthorized acquisition or acquisition without valid authorization of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a business.

Good faith acquisition of personal information by an employee or agent of the business for the purposes of the business is not a breach of the security of the system, provided that the private information is not used or subject to unauthorized disclosure.

Who does this law apply to?

Any person or business which conducts business in New York state, and which owns or licenses computerized data which includes private information or any person or business which maintains computerized data which includes private information which such person or business does not own.

Who must be notified?

Any resident of New York whose private information was or is reasonably believed to have been acquired by an individual without valid authorization must be notified.

The State Attorney General, the department of state, and the division of the state police must also be notified of the timing, content, and distribution of the notices as well as the approximate number of affected persons

If more than 5,000 New York residents are to be notified at one time, the person/business/entity must also notify consumer reporting agencies of the timing, content, and distribution of the notices as well as the approximate number of affected persons.

When must they be notified?

Notification should occur at the most expedient time possible without any unreasonable delay.

What must be included in the notification?

The following must be included in the notification: contact information for the person or business making the notification and a description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been acquired.

How must they be notified?

Written notice and electronic notice are permitted, provided that the person to whom notice is required has expressly consented to receiving said notice in electronic form and a log of each such notification is kept by the person or business who notifies affected persons in such form (consent to electronic notice cannot have been a condition to establishing a business relationship between the business/person and the persons to be notified).

Telephone notice is also allowed, provided that a log of each such notification is kept by the person or business who notifies affected persons

Substitute notice may be given if a business demonstrates to the state attorney general that the cost of providing notice would exceed $250,000, that the affected class of subject persons to be notified exceeds 500,000, or if such business does not have sufficient contact information.

Do any exceptions or exemptions apply?

Notification may be delayed if a law enforcement agency determines that such notification would impede a criminal investigation.

What are the legal consequences for violating the law?

A civil penalty of the greater of $5,000 or up to $10 per instance of failed notification not to exceed $150,000 is available.

NORTH CAROLINA

N.C. GEN. STAT §§ 75-61 – 65

What is a data breach?

A "security breach" is an incident of unauthorized access to and acquisition of unencrypted and unredacted records or data containing personal information where illegal use of the personal information has occurred or is reasonably likely to occur or that creates a material risk of harm to a consumer. Any incident of unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential process or key shall constitute a security breach.

Good faith acquisition of personal information by an employee or agent of the business for a legitimate purpose is not a security breach, provided that the personal information is not used for a purpose other than a lawful purpose of the business and is not subject to further unauthorized disclosure.

Who does this law apply to?

This law applies to any "business." A business includes any sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not

organized to operate at a profit. The term includes a financial institution organized, chartered, or holding a license or authorization certificate under the laws of this State, any other state, the United States, or any other country, or the parent or the subsidiary of any such financial institution. Business shall not include any government or governmental subdivision or agency.

Who must be notified?

Affected persons must be notified. The Consumer Protection Division of the Attorney General's Office must also be notified of the nature of the breach, the number of consumers affected by the breach, steps taken to investigate the breach, steps taken to prevent a similar breach in the future, and information regarding the timing, distribution, and content of the notice given to affected persons.

If more than 1,000 persons require notice at one time, the business must notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis

When must they be notified?

Notification should occur without unreasonable delay, consistent with the legitimate needs of law enforcement.

What must be included in the notification?

The attorney general's website contains a form to be used for notice. Notice must be "clear and conspicuous" and should include all of the following:

A description of the incident in general terms;

A description of the type of personal information that was subject to the unauthorized access and acquisition;

A description of the general acts of the business to protect the personal information from further unauthorized access;

A telephone number for the business that the person may call for further information and assistance, if one exists;

Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports;

The toll-free numbers and addresses for the major consumer reporting agencies; and

The toll-free numbers, addresses, and website addresses for the Federal Trade Commission and the North Carolina Attorney General's Office.

How must they be notified?

Written and electronic notice are permitted if the consumer has a valid email address and agreed to such electronic communications, so long as notice comports with the requirements of 15 U.S.C. § 7001. Telephonic notice is allowed provided that contact is made directly to affected persons.

Substitute notice is appropriate if the business demonstrates that the cost of providing notice would exceed $250,000, the affected class of subject persons to be notified exceeds 500,000, the business does not have sufficient contact information or consent to otherwise notify affected persons, or if the business is unable to identify particular affected persons.

Do any exceptions or exemptions apply?

Notice may be delayed if a law enforcement agency informs the business that notification

may impede a criminal investigation or jeopardize national or homeland security, provided that such request is made in writing or the business documents such request contemporaneously in writing, including the name of the law enforcement officer making the request and the officer's law enforcement agency engaged in the investigation.

What are the legal consequences for violating the law?

A violation of this section is a violation of G.S. 75-1.1. No private right of action may be brought by an individual for a violation of this section unless such individual is injured as a result of the violation.

NORTH DAKOTA

N.D. CENT. CODE § 51-30-01 – § 51-30-07 *et seq.*

What is a data breach?

"Breach of the security system" means the unauthorized acquisition of computerized data when access to personal information has not been secured by encryption or by any other method or technology that renders the electronic files, media, or databases unreadable or unusable.

Good faith acquisition of personal information by an employee or agent of the person is not a breach of the security of the system, if the personal information is not used or subject to further unauthorized disclosure.

Who does this law apply to?

The law applies to any person that conducts business in this state, and that owns or licenses computerized data that includes personal information.

Who must be notified?

Any person whose data has been compromised must be notified. Any person that maintains computerized data that includes personal information that the person does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following the discovery, if the personal information was, or is reasonably believed to have been acquired by an unauthorized agent.

When must they be notified?

Notification must occur in the most expedient time possible without undue delay.

What must be included in the notification?

Any breach of the security of the system must be included in the notification.

How must they be notified?

Notification is permitted through written notice and electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001.

Substitute notice is allowed, if the person demonstrates that the cost of providing notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000, or the person does not have sufficient contact information.

Do any exceptions or exemptions apply?

A person that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this chapter is deemed to be in compliance with the notification requirements of this chapter if the person notifies subject individuals in accordance with its policies in the event of a breach of security of the system. A financial institution, trust company, or credit union that is subject to, examined for, and in compliance with the federal interagency guidance on response programs for unauthorized access to customer information and customer notice is in compliance with this chapter.

Notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The required notification must be made after the law enforcement agency determines that the notification will not compromise the investigation.

What are the legal consequences for violating the law?

The attorney general may enforce this chapter.

OHIO

OHIO REV. CODE § 1349.19 *et seq*.

What is a data breach?

"Breach of the security of the system" is the unauthorized access to and acquisition of computerized data that compromises the security or confidentiality of personal information owned or licensed by a person and that causes, reasonably is believed to have caused, or reasonably is believed will cause a material risk of identity theft or other fraud to the person or property of a resident of this state.

Good faith acquisition of personal information by an employee or agent of the person for the purposes of the person is not a breach of the security of the system, provided that the personal information is not used for an unlawful purpose or subject to further unauthorized disclosure.

The acquisition of personal information pursuant to a search warrant, subpoena, or other court order, or pursuant to a subpoena, order, or duty of a regulatory state agency, is not a breach of the security of the system.

Who does the law apply to?

The law applies to any person or business entity that owns or licenses computerized data that includes personal information in the state of Ohio and to any person that, on behalf of or at the direction of another person or on behalf of or at the direction of any governmental entity, is the custodian of or stores computerized data that includes personal information

A business entity is any sole proprietorship, partnership, corporation, association, or other group, however organized under the laws of any state or country.

Who must be notified?

Following the discovery or notification of a data breach, the person or business must notify every Ohio resident whose personal information was or is reasonably believed to have been, acquired by an unauthorized person.

A resident of Ohio is an individual whose principal mailing address as reflected in the records of the person is in the state.

If more than 1,000 people must be notified in a single occurrence, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis must be notified of timing, distribution, and content of the disclosure given by person to the residents of the state must be notified.

When must they be notified?

The notification must be sent out in the most expedient time and manner possible but no later than forty-five (45) days following the discovery or notification of the breach.

What must be included in the notification?

The content of the notification is not explicitly addressed in the statute.

How must they be notified?

A person may be notified by written notice; electronic notice, if the person's primary method of communication with the resident to whom the disclosure must be made is by electronic means; or telephone notice.

Do any exceptions or exemptions apply?

If a law enforcement agency determines that the disclosure or notification will impede a criminal investigation or jeopardize homeland or national security, the notification will only be sent out after the law enforcement agency determines that the notification will not compromise the investigation.

What are the legal consequences for violating the law?

The attorney general may conduct an investigation based on a complaint or his/her own inquiries if the attorney general has reason to believe that a state agency has not followed the statute.

OKLAHOMA

24 OKLA. STAT. § 161 *et seq*.

What is a data breach?

"Breach of the security of a system" means an unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information that is reasonably believed to have caused or will cause any resident of the state harm.

Who does the law apply to?

The law applies to any individual or entity that owns, licenses, or maintains computerized data that includes personal information. An entity includes corporations, business trusts, estates, partnerships, limited partnerships, limited liability partnerships, limited liability companies, associations, organizations, joint ventures, governments, government subdivisions, agencies, or instrumentalities, or any other legal entity, whether for profit or not-for-profit.

Who must to be notified?

Following discovery or notice of the breach, all residents of the state whose personal information was or is reasonably believed to been accessed must be notified.

When must they be notified?

Notice must be made without any unreasonable delay.

What must be included in the notification?

If the entity has its own notification procedures as part of an information privacy or security policy, if the notice follows the requirements, the notice will be sufficient.

How must they be notified?

The person must be notified through written notice to the postal address of record, telephone notice, or electronic notice.

Do any exceptions or exemptions apply?

Notice may be delayed if a law enforcement agency determines and advises that the notice will impede a criminal or civil investigation or homeland or national security.

What are the legal consequences for violating the law?

A violation of the act that results in injury or loss to the residents of Oklahoma may be enforced by the attorney general in an amount up to $150,000 per breach.

OREGON

OR. REV. STAT. §§ 646A.600 *et seq*.

What is a data breach?

A "breach of security" is an unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information that a person maintains.

Who does the law apply to?

The law applies to any person that owns, maintains or otherwise possesses data that includes a consumer's personal information that is used in the course of business, vocation, occupation or volunteer activities.

A person is any individual, private or public corporation, partnership, cooperative, association, estate, limited liability company, organization or other entity, whether or not organized to operate for profit, or a public body as defined in ORS 174.109.

Who must be notified?

Following the discovery or notification of a breach, any consumer whose personal information was included in the information that was breached must be notified.

If the breach affected more than 1,000 consumers, notification must be sent to all consumer reporting agencies that compile and maintain reports on consumers on a nationwide basis.

When must they be notified?

The notification must be made in the most expeditious time possible without unreasonable delay.

What must be included in the notification?

At a minimum, the notification must include a general description of the incident; the approximate date of the breach; the type of personal information that was obtained in the breach; contact information of the person subject to this law; contact information for the national consumer reporting agencies; and advice to the consumer to report suspected identity theft to law enforcement.

How must they be notified?

Notice must be written; by telephone if the contact is the person directly affected by the breach; or by electronic notice if the person's customary method of communication with the consumer is by electronic means.

Do any exceptions or exemptions apply?

Notice may be delayed if a law enforcement agency determines that the notification will be a hindrance to a criminal investigation and that agency has made a written request that the notification be delayed.

Notification is not required if, after an appropriate investigation or after consultation with relevant federal, state or local agencies for law enforcement, it is determined that no reasonable likelihood of harm to the consumer has or will result from the breach.

What are the legal consequences for violating the law?

If a person violates this law, the Director of the Department of Consumer and Business Services may order the person to cease and desist from the violation or require the person to pay compensation to the consumers injured by the violation.

PENNSYLVANIA

73 PA. STAT. § 2301 *et seq.*

What is a data breach?

"Breach of the security of the system" is the unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of personal information that could cause loss or injury to any resident of the Commonwealth, maintained by the entity.

Who does the law apply to?

This law applies to any entity that maintains, stores, or manages computerized data that includes personal information.

An entity includes individuals, sole proprietorships, partnerships, corporations, associations or other groups, however organized and whether or not organized to operate for profit, including financial institutions, organized, chartered or holding a license or authorized under the laws of the Commonwealth or any other state or country.

Who must be notified?

Any resident of the Commonwealth whose personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person must be notified. A resident of the Commonwealth may be determined to be an individual whose principal mailing address is in the Commonwealth.

When notice must be sent to more than 1,000 people at one time, the entity must also notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.

When must they be notified?

Notification must be sent without unreasonable delay.

What must be included in the notification?

If the entity maintains its own notification procedures as part of an information privacy or security policy for the treatment of personal information, if the notice is consistent with the policy, it will meet the standard of the statute.

How must they be notified?

Notification can be written and sent to the last known home address, by telephone if the customer can reasonably expect to receive the call, or e-mail if a prior business relationship existed and the person or entity has a valid email address for the individual.

Do any exceptions or exemptions apply?

If a law enforcement agency, in writing, with specific reference to this statute, states the notice will impede a criminal or civil investigation, notice can be delayed.

What are the legal consequences for violating the law?

Violation of this law shall be deemed an unfair or deceptive act or practice in violation of the Unfair Trade Practices and Consumer Protection Law. P.L. 1224, No. 387.

RHODE ISLAND

R.I. GEN. LAWS § 11- 49.2-1 *et seq*.

What is a data breach?

A "breach of the security of the system" is an unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity or personal information maintained by the state agency or person.

Who does the law apply to?

The law applies to any state agency or person that owns, maintains or licenses computerized data that includes personal information.

A person includes any individual, partnership, association, corporation or joint venture.

Who must be notified?

Following discovery or notification of the breach, all residents of Rhode Island whose unencrypted personal information was or is reasonably believed to have been acquired must be notified.

When must they be notified?

Notification must be sent in the most expedient time possible and without unreasonable delay. Reasonable measures to determine the scope of the breach and restore the reasonable integrity of the data system may be taken before sending out notifications.

What must be included in the notification?

If the entity maintains its own security breach procedures as part of an information security policy for the treatment of personal information, notice shall be deemed sufficient, if the notification is in accordance with the policy.

How must they be notified?

Notification may be provided by written notice or electronic notice, if the notice is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C § 7001.

Do any exceptions or exemptions apply?

Notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation.

Notification is not required if after an appropriate investigation, or after consultation with relevant law enforcement agencies, a determination is made that the breach has not and will not likely result in a significant risk of identity theft to the individuals whose personal information was acquired.

What are the legal consequences for violating the law?

Each violation of this law is a civil violation with a penalty of no more than $100 per occurrence and no more than $25,000 against one defendant.

SOUTH CAROLINA

S.C. CODE § 39-1-90

What is a data breach?

"Breach of the security of the system" is any unauthorized access to and acquisition of computerized data that was not rendered unusable through encryption, redaction, or other methods that compromises the security, confidentiality, or integrity of personal identifying information that has or is reasonable likely to cause material risk or harm to residents of the state.

Who does this law apply to?

The law applies to any person conducting business in the state, and owning or licensing computerized data or other data that includes personal identifying information, or maintaining computerized data or other data that includes personal identifying information that the person does not own.

A person includes any individual, partnership, association, corporation, or joint venture.

Who must be notified?

Any resident of the state whose personal identifying information, that was not rendered unusable through encryption, redaction, or other methods, was or is reasonably likely to have been acquired and caused or is reasonably believed to be harmed must be notified.

When notice must be sent to more than 1,000 people at one time, the entity must also notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.

When must they be notified?

Notification must be sent in the most expedient time possible and without unreasonable delay. Reasonable measures to determine the scope of the breach and restore the reasonable integrity of the data system may be taken before sending out notifications.

What must be included in the notification?

If the entity maintains its own security breach procedures as part of an information security policy for the treatment of personal information, notice shall be deemed to meet the requirements of the statute if the notification is in accordance with the policy.

How must they be notified?

Notification may be sent in writing; by electronic notice if the person's primary method of communication with the individual is by electronic means; or by telephone.

Do any exceptions or exemptions apply?

Notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation.

What are the legal consequences for violating the law?

If the law is violated, the injured party can file suit to recover damages for willful and knowing violations, actual damages resulting from the violation in cases of negligence, and attorney's fees.

A person that knowingly and willfully violates the law is subject to an administrative fine of $1,000 for each resident whose personal information was accessible by the breach.

TENNESSEE

TENN. CODE § 47-18-2107

What is a data breach?

"Breach of the security of the system" means any unauthorized acquisition of unencrypted computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the information holder.

Who does the law apply to?

The law applies to any "information holder." An information holder is any person or business that conducts business in the state or agency of the state of Tennessee or any political subdivisions, that own or license computerized data that includes personal information.

The law does not apply to any person who is subject to Title V of the Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102.1.

Who must be notified?

Following the discovery or notification of a breach, any resident of Tennessee whose unencrypted personal information was, or is reasonably believed to have been, acquired must be notified**.**

When notice must be sent to more than 1,000 people at one time, the entity must also notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.

When must they be notified?

Notification must be sent in the most expedient time possible and without unreasonable delay. Reasonable measures to determine the scope of the breach and restore the reasonable integrity of the data system may be taken before sending out notifications.

What must be included in the notification?

If the entity maintains its own security breach procedures as part of an information security policy for the treatment of personal information, notice shall be deemed to meet the requirements of the statute if the notification is in accordance with the policy.

How must they be notified?

Notification can be in writing or electronic form, provided it is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001.

Do any exceptions or exemptions apply?

Notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation.

What are the legal consequences for violating the law?

Any customer of an information holder who is a person or business entity, but who is not an agency of the state or any political subdivision of the state, and who is injured by a violation of this section, may institute a civil action to recover damages and to enjoin the person or business entity from further action in violation of this section.

The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under law.

TEXAS

TEX. BUS. & COM. CODE §§ 521.053 *et seq*.

What is a data breach?

"Breach of system security" is an unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information.

Who does the law apply to?

The law applies to any person who conducts business in the state and owns or licenses computerized data that includes sensitive personal information and to any person who maintains computerized data that includes sensitive personal information not owned by the person.

A person includes any individual, partnership, association, corporation, or joint venture.

Who must be notified?

Notifications must be sent to any individual whose sensitive personal information was or is reasonably believed to have been acquired by an unauthorized person.

When notice must be sent to more than 1,000 people at one time, the entity must also notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.

When must they be notified?

Notification of the breach must be sent immediately after discovery of the breach, if the sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

What must be included in the notification?

If the entity maintains its own security breach procedures as part of an information security policy for the treatment of personal information, notice shall be deemed to meet the requirements of the statute if the notification is in accordance with the policy.

How must they be notified?

Notification can be in writing or electronic form, provided it is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001.

Do any exceptions or exemptions apply?

Notice may be delayed at the request of a law enforcement agency that determines that the notification will impede a criminal investigation.

What are the legal consequences for violating the law?

A person who violates this chapter is liable to this state for a civil penalty of at least $2,000 but not more than $50,000 for each violation. The attorney general may bring an action to recover the civil penalty imposed under this subsection.

A person who fails to take reasonable action to comply with § 521.053(b) is liable to this state for a civil penalty of not more than $100 for each individual to whom notification is due under that subsection for each consecutive day that the person fails to take reasonable action to comply with that subsection. Civil penalties under this section may not exceed $250,000 for all

individuals to whom notification is due after a single breach. The attorney general may bring an action to recover the civil penalties imposed under this subsection.

If it appears to the attorney general that a person is engaging in, has engaged in, or is about to engage in conduct that violates this chapter, the attorney general may bring an action in the name of the state against the person to restrain the violation by a temporary restraining order or by a permanent or temporary injunction.

UTAH

UTAH CODE §§ 13-44-101 *et seq*.

What is a data breach?

"Breach of system security" is an unauthorized acquisition of computerized data maintained by a person that compromises the security, confidentiality, or integrity of personal information.

Who does this law apply to?

The law applies to a person who owns or licenses computerized data that includes personal information concerning a Utah resident and a person who maintains computerized data that includes personal information that the person does not own or license.

Who must be notified?

Any resident of the state of Utah whose personal information was or is reasonably believed to have been affected by the breach must be notified.

When must they be notified?

Following discovery or notification of a breach, a good faith, reasonable and prompt, investigation to determine the likelihood that the personal information has been or will be misused is conducted. If the investigation reveals misuse has occurred or is reasonably likely to occur, the notification will be sent in the most expedient time possible.

What must be included in the notification?

The content of the notification is not explicitly addressed in the statute.

How must they be notified?

Notification can be sent in writing by first class mail, electronically if the person's primary method of communication with the resident is by electronic means, by telephone or by publishing notice of the breach.

Do any exceptions or exemptions apply?

Notice may be delayed at the request of a law enforcement agency that determines that the notification will impede a criminal investigation.

What are the legal consequences for violating the law?

The attorney general may bring charges for violations of this statute. If the statute is violated, the entity can be subject to civil fines of no more than $2,500 a violation per consumer or $100,000 total.

VERMONT

9 V.S.A. §§ 2430, 2435

What is a data breach?

"Security breach" is any unauthorized acquisition of electronic data or a reasonable belief of an unauthorized acquisition of electronic data that compromises the security, confidentiality, or integrity of a consumer's personally identifiable information maintained by the data collector.

Who does the law apply to?

The law applies to any data collector that owns or licenses computerized personally identifiable information that includes personal information concerning a consumer and to any data collector that maintains or possesses computerized data containing personally identifiable information of a consumer that the data collector does not own or license.

A data collector is any state, state agency, political subdivision of the state, public and private university, privately and publicly held corporations, limited liability companies, financial institutions, retail operations, and any other entity that, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates, or otherwise deals with nonpublic personal information.

Who must be notified?

Any consumer whose personal information was acquired in the data breach must be notified.

When notice must be sent to more than 1,000 people at one time, the entity must also notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.

When must they be notified?

Notice must be sent out in the most expedient time possible, without unreasonable delay, and no later than 45 days after discovery or notification of the breach.

What must be included in the notification?

The notification must be clear and conspicuous. The notification must include what happened in general terms, the type of personal information that was the subject of the breach, what is being done to protect against further breaches, a telephone number that the consumer may call for further information, advice to review account statements for fraudulent activity, and the approximate date of the breach.

How must they be notified?

Notification can be sent in writing mailed to the consumer's residence, through electronic notice for those consumers whose data had been collected by email, or by telephone notice.

Do any exceptions or exemptions apply?

The notice may be delayed upon request of a law enforcement agency if the notification may impede a law enforcement investigation or national or homeland security.

Notification is not required if after an appropriate investigation or after consultation with relevant law enforcement agencies, a determination is made that the breach has not and will not

likely result in a significant risk of identity theft to the individuals whose personal information was acquired.

What are the legal consequences for violating the law?

The attorney general and state's attorneys have sole and full authority to investigate violations of this law and may seek remedies for violations.

VIRGINIA

VA. CODE § 18.2-186.6

What is a data breach?

"Breach of the security of the system" is any unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information.

Who does the law apply to?

Any individual or entity that maintains computerized data that includes personal information that the individual or entity does not own or license and to an individual or entity that owns or licenses computerized data that includes personal information.

An entity is any business trusts, corporation, estate, partnership, limited partnership, limited liability partnership, limited liability company, association, organization, joint venture, governmental subdivision, agency, instrumentality or any other legal entity, whether for profit or not for profit.

Who must be notified?

Notification, once discovered, must be sent to the office of the attorney general and any affected resident of the Commonwealth.

When notice must be sent to more than 1,000 people at one time, the entity must also notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.

When must they be notified?

Notification must be sent without unreasonable delay after discovery of the data breach.

What must be included in the notification?

If the entity maintains its own security breach procedures as part of an information security policy for the treatment of personal information, notice shall be deemed to meet the requirements of the statute if the notification is in accordance with the policy.

How must they be notified?

Notification can be sent in writing to the last known postal address, by telephone, or electronic notice.

Do any exceptions or exemptions apply?

The notice may be delayed upon request of a law enforcement agency if the notification may impede a law enforcement investigation or national or homeland security.

What are the legal consequences for violating the law?

The attorney general may bring an action to address violations of this section. The civil penalty may not exceed $150,000 per breach.

WASHINGTON

WASH. REV. CODE § 19.255.010 *et seq*.

What is a data breach?

"Breach of the security of the system" is the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business.

Who does this law apply to?

Any person or business that conducts business in the state and that owns or licenses computerized data that includes personal information or that maintains computerized data that includes personal information that the person or business does not own.

Who must be notified?

Following discovery or notification of the breach, notifications must be sent out to any resident of the state whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person.

When must they be notified?

Notification shall be made in the most expedient time possible and without unreasonable delay. Notification may wait until after measures are taken to determine the scope of the breach and restore the reasonable integrity of the data system.

What must be included in the notification?

If the entity maintains its own security breach procedures as part of an information security policy for the treatment of personal information, notice shall be deemed to meet the requirements of the statute if the notification is in accordance with the policy.

How must they be notified?

Notification can be sent in writing or by electronic notice, if the notice is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001.

Do any exceptions or exemptions apply?

The notice may be delayed upon request of a law enforcement agency if the notification may impede a law enforcement investigation or national or homeland security.

What are the legal consequences for violating the law?

Any customer injured by a violation of this section may institute a civil action to recover damages.

WEST VIRGINIA

W. VA. CODE § 46A-2A-101 *et seq*.

What is a data breach?

"Breach of the security of a system" is the unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity that has caused or will cause harm to any resident of the state.

Who does the law apply to?

The law applies to any individual or entity that owns or licenses computerized data that includes personal information and any individual or entity that maintains computerized data that includes personal information that the individual or entity does not own or license.

An entity is any business trust, corporation, estate, partnership, limited partnership, limited liability partnership, limited liability company, association, organization, joint venture, governmental subdivision, agency, or instrumentality or any other legal entity, whether for profit or not for profit.

Who must be notified?

Following discovery or notification of the breach, any resident of the state whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed by an unauthorized person must be informed.

When notice must be sent to more than 1,000 people at one time, the entity must also notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.

When must they be notified?

Notification must be sent in the most expedient time possible and without unreasonable delay. Reasonable measures to determine the scope of the breach and restore the reasonable integrity of the data system may be taken before sending out notifications.

What must be included in the notification?

The notification shall include a description of the information that has been accessed, a telephone number or website that may be used to contact the entity where the individual can learn more, and a toll-free contact number and addresses for the major credit reporting agencies and information on how to place a fraud alert.

If the entity maintains its own security breach procedures as part of an information security policy for the treatment of personal information, notice shall be deemed to meet the requirements of the statute if the notification is in accordance with the policy.

How must they be notified?

Notification can be written and sent to the postal address of the individual or can be electronic, if the notice is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001.

Do any exceptions or exemptions apply?

The notice may be delayed upon request of a law enforcement agency if the notification may impede a law enforcement investigation or national or homeland security.

What are the legal consequences for violating the law?

Failure to follow the statute is an unfair and deceptive act or practice and is punishable by a fine not to exceed $150,000.

WISCONSIN

WIS. STAT. § 134.98

What is a data breach?

No definition provided.

Who does the law apply to?

An entity whose principal place of business is located in the state or an entity that maintains or licenses personal information. An entity means a person, other than an individual, that conducts business in the state and maintains personal information in the ordinary course of business. An entity also includes any state and any office, department, independent agency, authority, institution, association, society, or other body in state government created or authorized to be created by the constitution or any law, including the legislature and the courts.

Who must be notified?

Following discovery or notification of the breach, any resident of the state whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed by an unauthorized person must be informed.

When must they be notified?

Notification must be sent within a reasonable time, not to exceed 45 days after the entity learns of the acquisition of personal information.

What must be included in the notification?

The notification shall indicate that the entity knows of the unauthorized acquisition of personal information pertaining to the subject of the personal information.

How must they be notified?

Notification can be sent by mail or by a method the entity has previously employed to communicate with the subject of the personal information.

Do any exceptions or exemptions apply?

The notice may be delayed upon request of a law enforcement agency if the notification may impede a law enforcement investigation or national or homeland security.

An entity is not required to provide notice of the acquisition of personal information if the acquisition of personal information does not create a material risk of identity theft or fraud to the subject of the personal information or if the personal information was acquired in good faith

by an employee or agent of the entity, if the personal information is used for a lawful purpose of the entity.

What are the legal consequences for violating the law?

Failure to comply with this law is not negligence or a breach of any duty, but may be evidence of negligence or a breach of a legal duty.

WYOMING

WYO. STAT. § 40-12-501 *et seq*.

What is a data breach?

"Breach of the security of the data system" is an unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal identifying information maintained by a person or business and causes or is reasonably believed to cause loss or injury to a resident of this state.

Who does this law apply to?

An individual or commercial entity that conducts business in Wyoming and that owns or licenses computerized data that includes personal identifying information about a resident of Wyoming or any person who maintains computerized data that includes personal identifying information on behalf of another business entity.

Who must be notified?

When the breach is discovered and it is determined that the misuse of personal information occurred or is reasonably likely to occur, the commercial entity shall give notice as soon as possible to the affected Wyoming residents.

When must they be notified?

Notice shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.

What must be included in the notification?

Notification shall include a toll-free number that the individual may use to contact the person collecting the data, from which the individual may learn the toll-free contact telephone numbers and addresses for the major credit reporting agencies.

How must they be notified?

Notification can be sent by written notice or e-mail notice.

Do any exceptions or exemptions apply?

Notification may be delayed if a law enforcement agency determines, in writing, that the notification may seriously impede a criminal investigation.

What are the legal consequences for violating the law?

The attorney general may bring an action in law or equity to address any violation of this section and for other relief that may be appropriate to ensure proper compliance with this section, to recover damages, or both.

FEDERAL DATA PRIVACY LAWS

SECTION 5 OF THE FEDERAL TRADE COMMISSION ACT
15 U.S.C. § 45

What is a data breach?

A data breach is any unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person or business.

Who does this law apply to?

The Federal Trade Commission ("FTC") is an independent agency of the United States government, established in 1914 by the Federal Trade Commission Act. Section 5 of the FTC Act, 15 U.S.C. § 45, grants the FTC power to investigate and prevent deceptive trade practices and prosecute companies that engage in deceptive or unfair privacy and data protection practices. Section 5(a) of the FTC Act provides that "unfair or deceptive acts or practices in or affecting commerce ... are ... declared unlawful." (15 U.S.C. § 45(a)(1)).

Who must be notified?

The FTC has issued the Safeguards Rule (16 C.F.R. § 314) that does not specify exact parameters for notification in the event of a data breach, but it does require the company to consider notifying consumers, law enforcement, and/or businesses in the event of a security breach, and to comply with the relevant state data breach notification laws.

What are the legal consequences for violating the law?

The FTC may seek civil penalties from any person or company that violates a rule "with actual knowledge or knowledge fairly implied on the basis of objective circumstances that such act is unfair or deceptive and is prohibited by such rule." The FTC will attempt to reach a negotiated settlement with an offending company, under which the company voluntarily agrees to refrain from the disputed practice, to take steps to remedy the situation, and potentially pay fines, restitution, or other penalties. The consent agreement can include notification of affected persons that is specifically tailored to the facts of the case. The agreement is put in the public record and comments are collected, and the FTC can make the agreement a final order with full force of the law.

THE GRAMM–LEACH–BLILEY ACT ("GLB")
a/k/a FINANCIAL SERVICES MODERNIZATION ACT OF 1999
Subtitle A: Disclosure of Nonpublic Personal Information
15 U.S.C. § 6801 *et seq.*

What is a data breach?

Any unauthorized disclosure of personally identifiable financial information that was given by a consumer to a financial institution resulting from any transaction with the consumer or any service performed for the consumer or otherwise obtained by the financial institution.

Who does this law apply to?

Companies "that offer financial products or services to individuals, like loans, financial or investment advice, or insurance," which includes non-bank mortgage lenders, real estate appraisers, loan brokers, financial or investment advisers, debt collectors, tax return preparers, banks, and real estate settlement service providers.

Who must be notified?

See the discussion of the Safeguards Rule (16 C.F.R. § 314), above.

THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT ("HIPAA")

45 C.F.R. PARTS 160, 162, AND 164

What is a data breach?

Pursuant to § 164.402, "breach" means the acquisition, access, use, or disclosure of protected health information ("PHI") in a manner not permitted under the HIPAA Privacy Standards, which compromises the security or privacy of the PHI.

PHI includes health and demographic information about an individual that is transmitted or maintained in any medium where the information is created or received by a health care provider, health plan, employer, or health care clearinghouse. It relates to the past, present, or future physical or mental health condition of an individual, protecting an individual's records post-mortem for a period of 50 years to the same extent that it protects a living individual's health information. It also relates to the provision of health care to a person, or payment for the provision of health care to a person.

Who does this law apply to?

HIPPA applies to health care providers who conduct covered health care transactions electronically, health plans, and health care clearinghouses. Specific examples includes doctors, nurses, hospitals, clinics, pharmacies, nursing homes, health insurance companies, HMOs, and government programs that pay for Medicare and Medicaid. It requires that these providers, referred to as "common entities," have safeguards in place to ensure the privacy of PHI. In addition, it requires these entities set forth the circumstances under which covered entities may use or disclose an individual's PHI. HIPPA also applies to "business associates," whose services are legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, and financial. Examples of business associates include third-party administrators who assist a health plan with claims processing, a CPA firm whose accounting services to a health care provider involve access to PHI, and attorneys who provide legal services to a health plan involving access to PHI.

It also gives individuals rights with respect to their personal PHI. These rights include the right to examine their personal health records, to request corrections to those records, and the assurance that their records are protected and disclosed only as permitted.

Who must be notified?

The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification to individuals following a breach of PHI. In addition to notifying individuals whose health records were compromised, the Secretary of Health and Human Services must also be notified, as explained below.

When must they be notified?

The number of individuals affected by the breach determines when the notification must be submitted to the Secretary of Health and Human Services. When a breach affects more than 500 individuals, a covered entity must provide the Secretary of Health and Human Services with notice of the breach without unreasonable delay. The notification must occur no later than 60 days from discovery of the breach, and this notice must be submitted electronically by following the link provided on the U.S. Department of Health & Human Services website and by completing all information required on the breach notification form.

For breaches that affect fewer than 500 individuals, a covered entity must provide the Secretary of Health and Human Services with notice of breaches within 60 days of the end of the calendar year in which the breaches were discovered. This notice must be submitted electronically by following the link provided on the U.S. Department of Health & Human Services website and by completing all information required on the breach notification form. A separate form must be completed for every breach that was discovered during the calendar year.

How must they be notified?

If a breach of PHI occurs, covered entities must provide notification of the breach to affected individuals, the Secretary of Health and Human Services, and in certain circumstances, to the media. In addition, business associates must notify covered entities if a breach occurs at or by the business associate.

Do any exceptions or exemptions apply?

In limited circumstances, a provider or provider group would be exempt from HIPPA privacy requirements: where the provider has less than 10 full-time employees and all claims transactions to all payors are made solely on paper (regardless of whether the provider participates in Medicare or not); or where the provider has a practice of any size, all claims transactions to all payors are made solely on paper and the practice does not participate in Medicare.

What are the legal consequences for violating the law?

Civil and criminal sanctions exist for HIPPA violations. Civil sanctions include $100 per violation per person up to a maximum of $25,000 per person, per year, per standard violated. In addition to civil liability, criminal sanctions include $25,000 to $250,000, and/or 1-10 years in prison for inappropriate use of PHI.