BakerHostetler

Alabama

Statute

Ala. Code § 8-38-1 et seq.

Covered Entities

An individual or entity conducting business in Alabama, or Alabama government agency, that acquires or uses personal information.

Quick Notes

- **Definition of Breach.** Unauthorized acquisition.
- **Notification Deadline.** Within 45 days upon a determination that a breach has occurred.
- **Regulatory Notice Required?** Yes, if the breach requires notification of 1,000 or more Alabama residents.
- **Risk of Harm Analysis?** Yes.
- **Applies to Paper Records?** No.

Definition of Personal Information

An individual's first name or first initial and last name in combination with one or more of the following:

- A non-truncated Social Security number or tax ID number.
- A non-truncated driver's license number, state-issued ID card number, passport number, military ID number, or other unique ID number issued on a government document used to verify the identity of a specific individual.
- A financial account number, including a bank account number, credit card number, or debit card number in combination with any security code, access code, password, expiration date, or PIN that is necessary to access the financial account or to conduct a transaction that will credit or debit the financial account.
- Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional.
- An individual's health insurance policy number or subscriber ID number and any unique identifier used by a health insurer to identify the individual.
- A username or e-mail address in combination with a password or security question and answer that would permit access to an online account affiliated with the covered entity that is reasonably likely to contain or is used to obtain sensitive, personally identifying information.

Definition of Breach

The unauthorized acquisition of data in electronic form containing personal information.

Individual Notice

Timing

As expeditiously as possible and without unreasonable delay, within 45 days upon a determination that a breach has occurred and is reasonably likely to cause substantial harm to the individuals to whom the information relates.

Content

- The date, estimated date, or estimated date range of the breach;
- A description of the personal information that was acquired;
- A general description of the actions taken to restore the security and confidentiality of the personal information involved in the breach;
- A general description of steps an affected individual can take to protect himself or herself from identity theft; and
- Information that the individual can use to contact the covered entity to inquire about the breach.

Method

- Written notice sent to the mailing address of the individual in the records of the covered entity; or
- E-mail notice sent to the e-mail address of the individual in the records of the covered entity.

Substitute Notice

Substitute notice is permitted if the covered entity demonstrates one of the following:

- Excessive cost:
  - Excessive cost to the covered entity relative to the resources of the covered entity; or
  - The cost to the covered entity exceeds $500,000.
- Lack of sufficient contact information for the individual required to be notified.
- The number of individuals to be notified exceeds 100,000 people.

Substitute notice shall consist of all of the following:

- A conspicuous notice on the Internet website of the covered entity, if the covered entity maintains a website, for a period of 30 days; and
- Notice in print and in broadcast media, including major media in urban and rural areas where the affected individuals reside.

An alternative form of substitute notice may be used with the approval of the Attorney General.

Credit Monitoring

Not required.

Consumer Reporting Agency Notice

Threshold

If the breach requires notification of 1,000 or more Alabama residents.

Timing

Without unreasonable delay.

Regulatory Notice

Regulator

The Attorney General of Alabama.

Threshold

If the breach requires notification of 1,000 or more Alabama residents.

Timing

As expeditiously as possible and without unreasonable delay, within 45 days upon a determination that a breach has occurred and is reasonably likely to cause substantial harm to the individuals to whom the information relates.

Exemptions/Exceptions

HIPAA Exemption

A covered entity subject to or regulated by HIPAA is exempt from Alabama's data breach notification statute as long as the entity does all of the following:

- Maintains procedures pursuant to HIPAA.
- Provides notice to affected individuals pursuant to HIPAA.
- Timely provides a copy of the notice to the Attorney General when the number of individuals the covered entity notified exceeds 1,000.

GLBA Exemption

A covered entity subject to or regulated by GLBA is exempt from Alabama's data breach notification statute as long as the covered entity does all of the following:

- Maintains procedures pursuant to GLBA.
- Provides notice to affected individuals pursuant GLBA.
- Timely provides a copy of the notice to the Attorney General when the number of individuals the covered entity notified exceeds 1,000.

Risk of Harm

Notice is not required if the breach is not reasonably likely to cause substantial harm to the individuals to whom the information relates.

Good Faith/Employee Acquisition

Good faith acquisition of personal information by an employee or agent of a covered entity is not a breach, unless the information is used for a purpose unrelated to the business or subject to further unauthorized use.

Encryption/Redaction

There is no breach when the information involved in the incident is truncated, encrypted, secured, or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable.

Penalties/Private Right of Action

Private Right of Action

None.

Penalties

Penalties may be assessed at the rate of $5,000 per day for each consecutive day that the covered entity fails to take reasonable action to comply with Alabama's data breach notification statute. Penalties shall not exceed $500,000 per breach.

BakerHostetler

Alaska

Statute

Alaska Stat. § 45.48.010 et seq.

Covered Entities

A person doing business, a state or local governmental agency (except for an agency of the judicial branch), or person with more than 10 employees who owns or licenses personal information in any form.

Quick Notes

- **Definition of Breach.** Unauthorized acquisition.
- **Notification Deadline.** In the most expeditious time possible and without unreasonable delay.
- **Regulatory Notice Required?** No.
- **Risk of Harm Analysis?** Yes.
- **Applies to Paper Records?** Yes.

Definition of Personal Information

An individual's first name or first initial and last name in combination with one or more of the following:

- Social Security number;
- Driver's license number or state identification card number;
- Financial account number, credit card number, or debit card number; or
- Passwords, personal identification numbers, or other access codes for financial accounts.

Definition of Breach

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 covered entity.

Individual Notice

Timing

In the most expeditious time possible and without unreasonable delay.

Content

None specified.

Method

- Written notice to the last known home address for the individual; or
- Electronic notice if the covered entity's primary method of communication with the Alaska 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 the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001 et seq.).

Substitute Notice

Substitute notice is permitted if the covered entity demonstrates one of the following:

- The cost of providing notice would exceed $150,000;
- The affected class of Alaska residents to be notified exceeds 300,000; or
- The covered entity does not have sufficient contact information.

Substitute notice shall consist of all of the following:

- E-mail notice when the covered entity has an e-mail address for the Alaska resident;
- Conspicuous posting of the notice on the covered entity's website, if the covered entity maintains one; and
- Notification to major statewide media.

Credit Monitoring

Not required.

Consumer Reporting Agency Notice

Threshold

If the breach requires notification of 1,000 or more Alaska residents.

Timing

Without unreasonable delay.

Regulatory Notice

Regulator

None.

Threshold

N/A

Timing

N/A

Exemptions/Exceptions

HIPAA Exemption

None.

GLBA Exemption

Alaska's breach notification statute does not apply to a covered entity that is subject to the GLBA.

Risk of Harm

Notification is not required if, after an appropriate investigation and after written notification to the Alaska Attorney General, the covered entity determines that there is a reasonable likelihood that the breach has not caused and will not cause harm to the consumers whose personal information has been acquired.

Good Faith/Employee Acquisition

Good faith acquisition of personal information by an employee or agent of a covered entity for a legitimate purpose is not a breach if the employee or agent does not use the personal information for a purpose unrelated to a legitimate purpose of the covered entity and does not make further unauthorized disclosure of the personal information.

Encryption/Redaction

There is no breach when the information involved in the incident was secured by encryption or redaction such that the data was unreadable or unusable.

Penalties/Private Right of Action

Private Right of Action

None.

Penalties

Governmental agencies are 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) and may be enjoined from further violations.

A violation of Alaska's breach notification statute is a per se "unfair or deceptive act or practice" under Alaska Stat. §§ 45.50.471-45.50.561 if the violator is not a government agency.

The covered entity is not subject to civil penalties imposed under Alaska Stat. § 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 under Alaska Stat. §§ 45.48.010-45.48.090, except that the total civil penalty may not exceed $50,000 and damages that may be awarded against the covered entity under Alaska Stat. § 45.50.531 are limited to actual economic damages that do not exceed $500.

BakerHostetler

Arizona

Statute

Ariz. Rev. Stat. § 18-551 et seq.

Covered Entities

A natural person, corporation, business trust, estate, trust, partnership, association, joint venture, government or governmental subdivision or agency, or any other legal or commercial entity that conducts business in this state and that owns, maintains, or licenses unencrypted and unredacted, computerized personal information.

Quick Notes

- **Definition of Breach.** Unauthorized acquisition and access.
- **Notification Deadline.** Within 45 days of the determination of the breach.
- **Regulatory Notice Required?** Yes, if the breach requires notification of 1,000 or more Arizona residents.
- **Risk of Harm Analysis?** Yes.
- **Applies to Paper Records?** No.

Definition of Personal Information

An individual's first name or first initial and last name in combination with one or more of the following:

- An individual's Social Security number;
- The number on an individual's driver's license or non-operating identification license;
- A private key that is unique to an individual and that is used to authenticate or sign an electronic record;
- An individual's financial account number or credit or debit card number in combination with any required security code, access code, or password that would allow access to the individual's financial account;
- An individual's health insurance identification number;
- Information about an individual's medical or mental health treatment or diagnosis by a healthcare professional;
- An individual's passport number;
- An individual's taxpayer identification number or an identity protection personal identification number issued by the United States Internal Revenue Service (IRS);
- Unique biometric data generated from a measurement or analysis of human body characteristics to authenticate an individual when the individual accesses an online account; or
- An individual's username or e-mail address in combination with a password or security question and answer that allows access to an online account.

Definition of Breach

Unauthorized acquisition and access of data in electronic form containing personal information.

Individual Notice

Timing

Within 45 days after the determination that there has been a breach.

Content

- The approximate date of the breach;
- A brief description of the personal information included in the breach;
- The toll-free numbers and addresses for the three largest nationwide consumer reporting agencies; and
- The toll-free number, address, and website address for the Federal Trade Commission or any federal agency that assists consumers with identity theft matters.

Method

- Written notice sent to the mailing address of the individual;
- E-mail notice sent to the e-mail address of the individual; or
- Telephone, if telephonic contact is made directly with the affected individuals and prerecorded.

Substitute Notice

Substitute notice is permitted if the covered entity demonstrates one of the following:

- The cost of providing notice would exceed $50,000;
- The affected class of subject persons to be notified exceeds 100,000; or
- The covered entity does not have sufficient contact information.

Substitute notice shall consist of all the following:

- A written letter to the attorney general that demonstrates the facts necessary for substitute notice; and
- Conspicuous posting of the notice for at least 45 days on the website of the covered entity, if the covered entity maintains one.

Credit Monitoring

Not required.

Consumer Reporting Agency Notice

Threshold

If the breach requires notification of 1,000 or more Arizona residents.

Timing

None specified.

Regulatory Notice

Regulator

The Attorney General of Arizona and the Director of the Arizona Department of Homeland Security.

Threshold

If the breach requires notification of 1,000 or more Arizona residents.

Timing

No later than 45 days after the determination that there has been a breach.

Exemptions/Exceptions

HIPAA Exemption

Arizona's breach notification statute does not apply to a covered entity or business associate as defined under regulations implementing HIPAA.

GLBA Exemption

Arizona's breach notification statute does not apply to a covered entity that is subject to Title V of the GLBA.

Risk of Harm

Notice is not required if the covered entity, an independent third-party forensic auditor, or a law enforcement agency determines after a reasonable investigation that the breach has not resulted in, or is not reasonably likely to result in, substantial economic loss to affected individuals.

Good Faith/Employee Acquisition

Good faith acquisition of personal information by an employee or agent of the covered entity does not constitute a security system breach, provided that the information is not used for a purpose unrelated to the covered entity and is not subject to further unauthorized disclosure.

Encryption/Redaction

There is no breach when the information involved in the incident was secured by encryption or redaction such that the data was unreadable or unusable.

Penalties/Private Right of Action

Private Right of Action

None.

Penalties

A knowing and willful violation is an unlawful trade practice, and only the Arizona Attorney General may enforce a violation of Arizona's data breach notification statute. The Arizona Attorney General may impose a civil penalty for a violation of Arizona's data breach notification statute, not to exceed the lesser of $10,000 per affected individual or the total amount of economic loss sustained by affected individuals, but the maximum civil penalty from a breach or series of related breaches may not exceed $500,000.

BakerHostetler

Arkansas

Statute

Ark. Code Ann. § 4-110-101 et seq.

Covered Entities

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

Quick Notes

- **Definition of Breach.** Unauthorized acquisition.
- **Notification Deadline.** In the most expedient time and manner possible and without unreasonable delay.
- **Regulatory Notice Required?** Yes, if the breach requires notification of 1,000 or more Arkansas residents.
- **Risk of Harm Analysis?** Yes.
- **Applies to Paper Records?** No.

Definition of Personal Information

An individual's first name or first initial and last name in combination with any one or more of the following:

- Social Security number;
- Driver's license number or Arkansas identification card number;
- Account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account;
- Medical information; or
- Biometric data.

Definition of Breach

Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a covered entity.

Individual Notice

Timing

In the most expedient time and manner possible and without unreasonable delay.

Content

None specified.

Method

- Written notification; or
- Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001 et seq.).

Substitute Notice

Substitute notice is permitted if the covered entity demonstrates one of the following:

- The cost of providing notice would exceed $250,000;
- The affected class of subject persons to be notified exceeds 500,000; or
- The covered entity does not have sufficient contact information.

Substitute notice shall consist of all of the following:

- E-mail notice when the covered entity has an e-mail address for the subject persons;
- Conspicuous posting of the notice on the covered entity's website, if the covered entity maintains one; and
- Notification by statewide media.

Credit Monitoring

Not required.

Consumer Reporting Agency Notice

Threshold

CRA notice not required.

Timing

N/A

Regulatory Notice

Regulator

The Attorney General of Arkansas.

Threshold

If the breach requires notification of 1,000 or more Arkansas residents.

Timing

At the same time the breach is disclosed to an affected individual or within 45 days after the covered entity determines that there is a reasonable likelihood of harm to the individuals, whichever occurs first.

Exemptions/Exceptions

HIPAA Exemption

The provisions of Arkansas's breach notification statute do not apply to a covered entity that is regulated by a state or federal law that provides greater protection to personal information and at least as thorough disclosure requirements for breaches than that provided by Arkansas's breach notification statute. Compliance with the state or federal law shall be deemed compliance with Arkansas's breach notification statute.

GLBA Exemption

The provisions of Arkansas's breach notification statute do not apply to a covered entity that is regulated by a state or federal law that provides greater protection to personal information and at least as thorough disclosure requirements for breaches than that provided by Arkansas's breach notification statute. Compliance with the state or federal law shall be deemed compliance with Arkansas's breach notification statute.

Risk of Harm

Notice is not required if, after a reasonable investigation, the covered entity determines that there is no reasonable likelihood of harm to customers.

Good Faith/Employee Acquisition

The good faith acquisition of personal information by an employee or agent of the covered entity for the legitimate purposes of the covered entity is not considered a “breach” if the personal information is not otherwise used or subject to further unauthorized disclosure.

Encryption/Redaction

There is no breach when the information involved in the incident is encrypted or redacted such that it is unreadable or unusable.

Penalties/Private Right of Action

Private Right of Action

None.

Penalties

Any violation of Arkansas’s breach notification statute is punishable by action of the Attorney General as a deceptive trade practice.

BakerHostetler

California

Statute

Cal. Civ. Code §1798.82 et seq.

Covered Entities

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

Quick Notes

- **Definition of Breach.** Unauthorized acquisition.
- **Notification Deadline.** Within 30 days of discovery or notification of the incident.
- **Regulatory Notice Required?** Yes, if the breach requires notification to 500 or more California residents.
- **Risk of Harm Analysis?** No.
- **Applies to Paper Records?** No.

Definition of Personal Information

An individual's first name or first initial and last name in combination with any one or more of the following:

- Social Security number;
- Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual;
- Account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account;
- Medical information (any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional);
- Health insurance information (an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records);
- Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes;

- Information or data collected through the use or operation of an automated license plate recognition system;
- Genetic data (any data, regardless of its format, that results from the analysis of a biological sample of an individual, or from another source enabling equivalent information to be obtained, and concerns genetic material. Genetic material includes, but is not limited to, DNA, RNA, genes, chromosomes, alleles, genomes, alterations or modifications to DNA or RNA, single nucleotide polymorphisms, uninterpreted data that results from analysis of the biological sample or other source, and any information extrapolated, derived, or inferred therefrom); or
- A username or e-mail address in combination with a password or security question and answer that would permit access to an online account.

Definition of Breach

Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business.

Individual Notice

Timing

In the most expedient time possible and without unreasonable delay.

Content

- The name and contact information of the reporting person or business subject to this section;
- A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;
- If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice;
- Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided;
- A general description of the breach incident, if that information is possible to determine at the time the notice is provided; and
- The toll-free telephone numbers and addresses of the major credit reporting agencies, if the breach exposed a social security number or a driver's license or California identification card number.

The notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information."

Method

- Written notice; or
- Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001 et seq.).

Substitute Notice

Substitute notice is permitted if the covered entity demonstrates one of the following:

- The cost of providing notice would exceed $250,000;
- The affected class of subject persons to be notified exceeds 500,000; or
- The covered entity does not have sufficient contact information.

Substitute notice shall consist of all of the following:

- E-mail notice when the covered entity has an e-mail address for the subject persons;
- Conspicuous posting of the notice on the covered entity's website, if the covered entity maintains one; and
- Notification to major statewide media.

Credit Monitoring

Not required. If offered, however, credit monitoring shall be provided at no cost for not less than 12 months to any person whose Social Security number and/or driver's license number was or may have been breached.

Consumer Reporting Agency Notice

Threshold

No CRA notice requirement.

Timing

N/A

Regulatory Notice

Regulator

The Attorney General of California.

Threshold

If the breach requires notification of 500 or more California residents.

Timing

Within 15 days of notifying consumers of the incident.

Exemptions/Exceptions

HIPAA Exemption

California's breach notification statute deems entities covered by HIPAA in compliance with the content requirements for individual notices if they have complied with the notice content requirements in the HITECH Act (42 U.S.C. 17932).

GLBA Exemption

None.

Risk of Harm

None.

Good Faith/Employee Acquisition

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

Encryption/Redaction

California's breach notification statute does not apply to information that is encrypted or rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security.

Penalties/Private Right of Action

Private Right of Action

Any customer injured by a violation of California's breach notification statute may institute a civil action to recover damages.

Penalties

Cal. Civ. Code § 1798.84 allows for a penalty not to exceed $3,000 per violation for a willful, intentional, or reckless violation; otherwise, a civil penalty of up to $500 per violation.

BakerHostetler

Colorado

Statute

Colo. Rev. Stat. § 6-1-716

Covered Entities

An individual or commercial entity that maintains, owns, or licenses computerized data that includes personal information about a resident of Colorado.

Quick Notes

- **Definition of Breach.** Unauthorized acquisition.
- **Notification Deadline.** 30 days from the date of determination that a security breach occurred.
- **Regulatory Notice Required?** Yes, if a breach requires notification to 500 or more Colorado residents.
- **Risk of Harm Analysis?** Yes.
- **Applies to Paper Records?** No.

Definition of Personal Information

A Colorado resident's first name or first initial and last name in combination with any one or more of the following:

- Social Security number;
- Student, military, or passport identification number;
- Driver's license number or identification card number;
- Medical information (any information about a consumer's medical or mental health treatment or diagnosis by a healthcare professional);
- Health insurance identification number or biometric data (unique biometric data generated from measurements or analysis of human body characteristics for the purpose of authenticating the individual when he or she accesses an online account);
- Username or e-mail address in combination with a password or security questions and answers that would permit access to an online account; or
- Account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to that account.

Definition of Breach

Unauthorized acquisition of unencrypted, computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a covered entity.

Individual Notice

Timing

In the most expedient time possible and without unreasonable delay, but not later than 30 days after the date of determination that a security breach occurred.

Content

Notice shall include the following:

- The date, estimated date, or estimated date range of the security breach;
- A description of the personal information that was acquired or reasonably believed to have been acquired as part of the security breach;
- Information that the resident can use to contact the covered entity to inquire about the security breach;
- The toll-free numbers, addresses, and websites for consumer reporting agencies;
- The toll-free number, address, and website for the Federal Trade Commission; and
- A statement that the resident can obtain information from the Federal Trade Commission and the credit reporting agencies about fraud alerts and security freezes.

Method

- Written notice to the postal address listed in the records of the covered entity;
- Telephonic notice; or
- Electronic notice, if the notice provided is consistent with the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001 et seq.).

Substitute Notice

Substitute notice is permitted if the covered entity demonstrates one of the following:

- The cost of providing notice would exceed $250,000;
- The affected class of subject persons to be notified exceeds 250,000 Colorado residents; or
- The covered entity does not have sufficient contact information.

Substitute notice shall consist of all of the following:

- E-mail notice when the covered entity has an e-mail address for the Colorado resident;
- Conspicuous posting of the notice on the covered entity's website, if the covered entity maintains one; and
- Notification to major statewide media.

Credit Monitoring

Not required.

Consumer Reporting Agency Notice

Threshold

If the breach requires notification of 1,000 or more Colorado residents.

Timing

Without unreasonable delay.

Regulatory Notice

Regulator

The Attorney General of Colorado.

Threshold

If a breach requires notification of 500 or more Colorado residents.

Timing

In the most expedient time possible and without unreasonable delay, but not later than 30 days after the date of determination that a security breach occurred.

Exemptions/Exceptions

HIPAA Exemption

A covered entity that is regulated by state or federal law and that maintains procedures for a security breach pursuant to the laws, rules, regulations, guidance, or guidelines established by its state or federal regulator is in compliance with Colorado's breach notification statute; except that notice to the Colorado Attorney General is still required pursuant to Regulatory Notice subsection if a breach requires notification to 500 or more Colorado residents. In the case of a conflict between the time period for notice to individuals that is required pursuant to Colorado's breach notification statute and the applicable state or federal law or regulation, the law or regulation with the shortest time frame for notice to the individual controls.

GLBA Exemption

A covered entity that is regulated by state or federal law and that maintains procedures for a security breach pursuant to the laws, rules, regulations, guidance, or guidelines established by its state or federal regulator is in compliance with Colorado's breach notification statute; except that notice to the Colorado Attorney General is still required pursuant to Regulatory Notice subsection if a breach requires notification to 500 or more Colorado residents. In the case of a conflict between the time period for notice to individuals that is required pursuant to Colorado's breach notification statute and the applicable state or federal law or regulation, the law or regulation with the shortest time frame for notice to the individual controls.

Risk of Harm

Notification is not required if an investigation determines that the misuse of information about a Colorado resident has not occurred or is not reasonably likely to occur.

Good Faith/Employee Acquisition

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

Encryption/Redaction

There is no breach when the information involved in the incident was secured by encryption such that it was unreadable or unusable.

Penalties/Private Right of Action

Private Right of Action

None.

Penalties

The Colorado Attorney General may bring an action in law or equity to address violations of Colorado's breach notification statute and for other relief that may be appropriate to ensure compliance with the statute or to recover direct economic damages resulting from a violation, or both.

BakerHostetler

Connecticut

Statute

Conn. Gen. Stat. § 36a-701b

Covered Entities

An individual or entity conducting business in Connecticut that owns, licenses, or maintains computerized data that includes personal information.

Quick Notes

- **Definition of Breach.** Unauthorized access or acquisition.
- **Notification Deadline.** Within 60 days after the discovery of a breach.
- **Regulatory Notice Required?** Yes, if the breach requires notification of 1 or more Connecticut residents.
- **Risk of Harm Analysis?** Yes.
- **Applies to Paper Records?** No.

Definition of Personal Information

An individual's first name or first initial and last name in combination with any one or more of the following:

- Social Security number;
- Taxpayer identification number;
- Identity protection personal identification number issued by the IRS;
- Driver's license number, state identification card number, passport number, military identification number, or other identification number issued by the government that is commonly used to verify identity;
- Credit or debit card number;
- Financial account number in combination with any required security code, access code, or password that would permit access to such financial account;
- Medical information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional;
- Health insurance policy number or subscriber identification number, or any unique identifier used by a health insurer to identify the individual;
- Biometric information consisting of data generated by electronic measurements of an individual's unique physical characteristics used to authenticate or ascertain the individual's identity, such as a fingerprint, voice print, retina or iris image;
- Precise geolocation data; or

Username or electronic mail address in combination with a password or security question and answer that would permit access to an online account.

Definition of Breach

Unauthorized access to or unauthorized acquisition of electronic files, media, databases, or computerized data containing personal information.

Individual Notice

Timing

Without unreasonable delay, but not later than 60 days after the discovery of a breach.

Content

For Connecticut residents whose Social Security number or taxpayer identification number was involved in the breach: information on how such resident can place a credit freeze on their credit file.

Method

- Written notice;
- Telephone notice; or
- Electronic notice, if the notice provided is consistent with the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001 et seq.).

Substitute Notice

Substitute notice is permitted if the covered entity demonstrates one of the following:

- The cost of providing direct notice would exceed $250,000;
- The affected class of subject persons to be notified exceeds 500,000 persons; or
- The covered entity does not have sufficient contact information.

Substitute notice shall consist of all of the following:

- E-mail notice when the covered entity has an e-mail address for the affected persons;
- Conspicuous posting of the notice on the website of the covered entity, if the covered entity maintains one; and
- Notification to major statewide media, including newspapers, radio, and television.

Credit Monitoring

Required at no cost for a period of not less than 24 months for Connecticut residents whose Social Security number or taxpayer identification number was involved in the breach.

Consumer Reporting Agency Notice

Threshold

CRA notice not required.

Timing

N/A

Regulatory Notice

Regulator

Attorney General of Connecticut.

Threshold

If the breach requires notification of 1 or more Connecticut residents.

Timing

Not later than the time when notice is provided to the Connecticut resident.

Exemptions/Exceptions

HIPAA Exemption

A covered entity that is subject to and in compliance with the privacy and security standards under HIPAA shall be deemed to be in compliance with Connecticut's breach notification statute, provided that they also provide notice to the Attorney General not later than the time when notice is provided to residents if notification to the Attorney General would otherwise be required, and that the covered entity complies with the credit monitoring requirement.

GLBA Exemption

A covered entity that maintains procedures pursuant to GLBA shall be deemed to be in compliance with Connecticut's breach notification statute, provided that the covered entity notifies residents in accordance with GLBA and also notifies the Attorney General not later than the time when notice is provided to the Connecticut resident.

Risk of Harm

Notification is not required if, after an appropriate investigation, the covered entity reasonably determines that the breach will not likely result in harm to the individuals whose personal information has been acquired or accessed.

Good Faith/Employee Acquisition

None specified.

Encryption/Redaction

There is no breach when personal information has been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable.

Penalties/Private Right of Action

Private Right of Action

None.

Penalties

Failure to comply with Connecticut's breach notification statute shall constitute an unfair trade practice and shall be enforced by the Attorney General. The Attorney General can recover civil penalties for violations of Connecticut's breach notification statute.

BakerHostetler

Delaware

Statute

Del. Code Ann. tit. 6 § 12B-101 et seq.

Covered Entities

Any individual or entity who conducts business in Delaware and who owns or licenses computerized data that includes personal information.

Quick Notes

- **Definition of Breach.** Unauthorized acquisition.
- **Notification Deadline.** Not later than 60 days after determination of the breach.
- **Regulatory Notice Required?** Yes, if notifying 500 or more Delaware residents.
- **Risk of Harm Analysis?** Yes.
- **Applies to Paper Records?** No.

Definition of Personal Information

An individual's first name or first initial and last name in combination with one or more of the following:

- Social Security number;
- Driver's license number or state or federal identification card number;
- Account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to a resident's financial account;
- Passport number;
- Username or e-mail address in combination with a password or security question and answer that would permit access to an online account;
- Medical history, medical treatment by a healthcare professional, diagnosis of mental or physical condition by a healthcare professional, or DNA profile;
- Health insurance policy number, subscriber identification number, or any other unique identifier used by a health insurer to identify the person;
- Unique biometric data generated from measurements or analysis of human body characteristics for authentication purposes; or
- Individual taxpayer identification number.

Definition of Breach

The unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information.

Individual Notice

Timing

Without unreasonable delay, but not later than 60 days after determination of the breach of security.

Content

If the breach affects an individual's Social Security number, the notice letter must include information necessary to enroll in the credit monitoring services and information about how the resident can place a credit freeze on their credit file.

Method

- Written notice;
- Telephonic notice; or
- Electronic notice for those consumers for whom the entity has a valid e-mail address and who have agreed to receive communications electronically, if the notice provided is consistent with the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001 et seq.) or if the covered entity's primary means of communication with the consumer is by electronic means.

Substitute Notice

Substitute notice is permitted if the covered entity demonstrates one of the following:

- The cost of providing notice would exceed $75,000; or
- The affected class of subject persons to be notified exceeds 100,000 Delaware residents; or
- The covered entity does not have sufficient contact information to provide notice.

Substitute notice shall consist of all of the following:

- E-mail notice when the covered entity has an e-mail address for the subject persons;
- Conspicuous posting of the notice on the covered entity's website, if the covered entity maintains one; and
- Notification to major statewide media.

Credit Monitoring

If the breach involves files containing an individual's Social Security number, the covered entity shall offer credit monitoring services at no cost for 1-year to each resident whose Social Security number was involved.

Consumer Reporting Agency Notice

Threshold

CRA notice not required.

Timing

N/A

Regulatory Notice

Regulator

The Delaware Attorney General.

Threshold

If the breach requires notification of 500 or more Delaware residents.

Timing

Concurrently with notice to individuals.

Exemptions/Exceptions

HIPAA Exemption

Any covered entity or business associate that is subject to and in compliance with the privacy and security standards for the protection of electronic personal health information established under HIPAA and HITECH shall be deemed to be in compliance with Delaware's breach notification statute.

GLBA Exemption

A financial institution that complies with the notification requirements prescribed by the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice is deemed to be in compliance with Delaware's breach notification statute.

Risk of Harm

Notification is not required if, after an appropriate investigation, the covered entity reasonably determines that the breach of security is unlikely to result in harm to the individual whose personal information had been breached.

Good Faith/Employee Acquisition

Good faith acquisition of personal information by an employee or agent of the covered entity is not a breach if the personal information is not used for a purpose other than the lawful purpose of the covered entity and is not subject to further unauthorized disclosure.

Encryption/Redaction

There is no breach when the information involved in the incident was secured by encryption or by any other method that renders the data unreadable or unusable.

Penalties/Private Right of Action

Private Right of Action

None.

Penalties

The Delaware Attorney General may bring an action in law or equity to address violations of Delaware's breach notification statute.

BakerHostetler

District of Columbia

Statute

D.C. Code § 28-3851 et seq.

Covered Entities

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.

Quick Notes

- **Definition of Breach.** Unauthorized acquisition.
- **Notification Deadline.** Without unreasonable delay.
- **Regulatory Notice Required?** Yes, if the breach requires notification of 50 or more Washington D.C. residents.
- **Risk of Harm Analysis?** Yes.
- **Applies to Paper Records?** No.

Definition of Personal Information

An individual's first name or first initial and last name, or any other personal identifier, in combination with any of the following:

- Social Security number;
- Individual Taxpayer ID Number;
- Passport number;
- Driver's license number, District of Columbia ID number, military identification number, or other unique identification number created or collected by a government body;
- Account number, credit card number, or debit card number in combination with any required code or password that would permit access to an individual's financial or credit account;
- Medical information;
- Genetic information;
- Health insurance information;
- Biometric data
- A username or e-mail address in combination with a password or security question and answer, or other means of authentication, or any combination of the above data elements that permits access to an individual's e-mail account; or

Any combination of the above data elements that would enable a person to commit identity theft without reference to a person's first name or first initial and last name or other independent personal identifier.

Definition of Breach

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 covered entity.

Individual Notice

Timing

In the most expedient time possible and without unreasonable delay.

Content

The notice shall, at minimum, include:

- A description of the categories of information that were or are reasonably believed to have been acquired by an unauthorized person, including the elements of personal information that were or are reasonably believed to have been acquired;
- Contact information for the covered entity, including the business address, telephone number, and toll-free telephone number, if one is maintained;
- The toll-free telephone numbers and addresses for the major consumer reporting agencies, including a statement notifying the resident of the right to obtain a security freeze free of charge pursuant to 15 U.S.C. § 1681c-1 and information on how a resident may request a security freeze; and
- The toll-free telephone numbers, addresses, and website addresses for the following entities, including a statement that an individual can obtain information from these sources about steps to take to avoid identity theft:
  - The Federal Trade Commission; and
  - The Office of the Attorney General for the District of Columbia.

Method

- Written notice; or
- Electronic notice, if the notice provided is consistent with the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001 et seq.).

Substitute Notice

Substitute notice is permitted if the covered entity demonstrates one of the following:

- The cost of providing notice would exceed $50,000;
- The affected class of Washington D.C. residents to be notified exceeds 100,000; or
- The covered entity does not have sufficient contact information.

Substitute notice shall consist of the following:

- E-mail notice when the covered entity has an e-mail address for the Washington D.C. resident;
- Conspicuous posting of the notice on the covered entity's website, if the covered entity maintains one; and
- Notice to major local and, if applicable, national media.

Credit Monitoring

Complimentary credit monitoring shall be provided for a period of not less than 18 months for Washington D.C. residents whose Social Security number or tax identification number was involved in the breach.

Consumer Reporting Agency Notice

Threshold

If the breach requires notification of 1,000 or more Washington D.C. residents.

Timing

Without unreasonable delay.

Regulatory Notice

Regulator

The Attorney General for the District of Columbia.

Threshold

If the breach requires notification of 50 or more Washington D.C. residents.

Timing

In the most expedient manner possible, without unreasonable delay, and in no event later than when individual notice is provided.

Exemptions/Exceptions

HIPAA Exemption

A covered entity that maintains procedures for complying with the breach notification procedures established under HIPAA, and provides notice in accordance with HIPAA, is deemed to be in compliance with the Washington D.C. breach notification statute with respect to the notification of residents whose personal information is included in the breach.

GLBA Exemption

A covered entity that maintains procedures for a breach notification system under Title V of the GLBA, and provides notice in accordance with the GLBA, is deemed to be in compliance with the Washington D.C. breach notification statute.

Risk of Harm

Notification is not required if, after a reasonable investigation and consultation with the Office of the Attorney General for the District of Columbia and federal law enforcement agencies, the covered entity determines the incident will likely not result in harm to any Washington D.C. resident.

Good Faith/Employee Acquisition

Good faith acquisition of personal information by an employee or agent of the covered entity is not a breach if the personal information is not used for a purpose other than the lawful purpose of the covered entity and is not subject to further unauthorized disclosure.

Encryption/Redaction

There is no breach when the information involved in the incident was secured by encryption, redaction, or some other method or technology that rendered the data unreadable or unusable.

Penalties/Private Right of Action

Private Right of Action

Washington D.C.'s breach notification statute provides for private rights of action for consumers who have been harmed by violations of the statute.

Penalties

A violation of the Washington D.C. breach notification statute is an unfair or deceptive trade practice, which can result in the assessment of civil penalties.

important decision that should not be based solely upon advertisements. Before you decide, ask us to send you written information about our qualifications and experience.

BakerHostetler

Florida

Statute

Fla. Stat. § 501.171

Covered Entities

An individual or entity conducting business in Florida that acquires, maintains, stores, or uses personal information.

Quick Notes

- **Definition of Breach.** Unauthorized access.
- **Notification Deadline.** Within 30 days after the determination of a breach or reason to believe a breach occurred.
- **Regulatory Notice Required?** Yes, if the breach requires notification of 500 or more Florida residents.
- **Risk of Harm Analysis?** Yes.
- **Applies to Paper Records?** No.

Definition of Personal Information

An individual's first name or first initial and last name in combination with one or more of the following:

- Social Security number;
- Driver license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity;
- Financial account number or credit or debit card number in combination with any required security code, access code, or password that is necessary to permit access to an individual's financial account;
- Information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional;
- An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual;
- An individual's biometric data;
- Any information regarding an individual's geolocation; or
- A username or e-mail address in combination with a password or security question and answer that would permit access to an online account.

Definition of Breach

Unauthorized access to data in electronic form containing personal information.

Individual Notice

Timing

No later than 30 days after the determination of a breach or reason to believe a breach occurred.

Content

- The date, estimated date, or estimated date range of the breach;
- A description of the personal information that was accessed or reasonably believed to have been accessed as a part of the breach; and
- Information that the individual can use to contact the covered entity to inquire about the breach and the personal information that the covered entity maintained about the individual.

Method

- Written notice sent to the mailing address of the individual; or
- E-mail notice sent to the e-mail address of the individual.

Substitute Notice

Substitute notice is permitted if the covered entity demonstrates one of the following:

- The cost of providing notice would exceed $250,000;
- The number of affected individuals exceeds 500,000 persons; or
- The covered entity does not have an e-mail address or mailing address for the affected individuals.

Substitute notice shall consist of all of the following:

- Conspicuous notice on the website of the covered entity, if the covered entity maintains a website; and
- Notice is published in print and to broadcast media, including major media in urban and rural areas where the affected individuals reside.

Credit Monitoring

Not required.

Consumer Reporting Agency Notice

Threshold

If the breach requires notification of 1,000 or more Florida residents.

Timing

Without unreasonable delay.

Regulatory Notice

Regulator

The Florida Department of Legal Affairs.

Threshold

If the breach requires notification of 500 or more Florida residents.

Timing

No later than 30 days after the determination of the breach or reason to believe a breach occurred.

Exemptions/Exceptions

HIPAA

Notice provided pursuant to HIPAA is deemed to be in compliance with Florida's breach notification statute if the covered entity notifies affected individuals in accordance with HIPAA in the event of a breach. A covered entity that timely provides a copy of such notice to the Florida Department of Legal Affairs is deemed to be in compliance with the regulatory notice requirement of Florida's breach notification statute.

GLBA

Notice provided pursuant to GLBA is deemed to be in compliance with Florida's breach notification statute if the covered entity notifies affected individuals in accordance GLBA in the event of a breach. A covered entity that

timely provides a copy of such notice to the Florida Department of Legal Affairs is deemed to be in compliance with the regulatory notice requirement of Florida's breach notification statute.

Risk of Harm

Notice is not required if, after an appropriate investigation and consultation with relevant federal, state, or local law enforcement agencies, the covered entity reasonably determines that the breach has not and will not likely result in identity theft or any other financial harm to the individuals whose personal information has been accessed. Such a determination must be documented in writing and maintained for at least five years. The covered entity shall provide the written determination to the Florida Department of Legal Affairs within 30 days after the determination.

Good Faith/Employee Acquisition

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 covered entity or subject to further unauthorized use.

Encryption/Redaction

There is no breach when the information involved in the incident is encrypted, secured, or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable.

Penalties/Private Right of Action

Private Right of Action

None.

Penalties

A violation of Florida's breach notification statute is deemed to be an unfair or deceptive trade practice. The Florida Department of Legal Affairs can bring an action for civil penalties, calculated as follows:

- In the amount of $1,000 for each day up to the first 30 days that notice was late and, thereafter, $50,000 for each subsequent 30-day period or portion thereof for up to 180 days.
- If the violation continues for more than 180 days, in an amount not to exceed $500,000.

The civil penalties apply per breach and not per individual affected by the breach.

BakerHostetler

Georgia

Quick Notes

- **Definition of Breach.** Unauthorized acquisition.
- **Notification Deadline.** Without unreasonable delay.
- **Regulatory Notice Required?** No.
- **Risk of Harm Analysis?** No.
- **Applies to Paper Records?** No.

Statute

Ga. Code § 10-1-910 et seq.

Covered Entities

- "Information Brokers," which refers to any person or entity who, for monetary fees or dues, engages, in whole or in part, in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring, or communicating information concerning individuals for the primary purpose of furnishing personal information to nonaffiliated third parties, but does not include any governmental agency whose records are maintained primarily for traffic safety, law enforcement, or licensing purposes; and
- "Data Collectors," which refers to any state or local agency or subdivision thereof, including any department, bureau, authority, public university or college, academy, commission, or other government entity; provided, however, that the term "data collector" does not include any governmental agency whose records are maintained primarily for traffic safety, law enforcement, licensing purposes, or for purposes of providing public access to court records or to real or personal property information.

Definition of Personal Information

An individual's first name or first initial and last name in combination with any one or more of the following:

- Social Security number;
- Driver's license number or state identification card number;
- Account number, credit card number, or debit card number, if circumstances exist wherein such a number could be used without additional identifying information, access codes, or passwords;
- Account passwords or personal identification numbers or other access codes; or
- Any of the previously listed items when not in connection with the individual's first name or first initial and last name, if the information compromised would be sufficient to perform or attempt to perform identity theft against the person whose information was compromised.

Definition of Breach

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.

Individual Notice

Timing

An information broker or data collector that maintains computerized data that includes personal information of individuals must, without unreasonable delay, notify individuals of a breach that involves their personal information.

Any person or business that maintains computerized data on behalf of an information broker or data collector, that includes personal information of individuals that the person or business does not own, shall notify the information broker or data collector of any breach within 24 hours following discovery.

Content

None specified.

Method

- Written notice;
- Telephone notice; or
- Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001 et seq.).

Substitute Notice

Substitute notice is permitted if the covered entity demonstrates one of the following:

- The cost of providing notice would exceed $50,000;
- The affected class of subject persons to be notified exceeds 100,000; or
- The covered entity does not have sufficient contact information.

Substitute notice shall consist of all of the following:

- E-mail notice when the covered entity has an e-mail address for the subject persons;
- Conspicuous posting of the notice on the covered entity's website, if the covered entity maintains one; and
- Notification to major statewide media.

Credit Monitoring

Not required.

Consumer Reporting Agency Notice

Threshold

If the breach requires notification of 10,000 or more Georgia residents.

Timing

Without unreasonable delay.

Regulatory Notice

Regulator

None.

Threshold

N/A

Timing

N/A

Exemptions/Exceptions

HIPAA Exemption

None.

GLBA Exemption

None.

Risk of Harm

None.

Good Faith/Employee Acquisition

Good faith acquisition or use of personal information by an employee or agent of an information broker or data collector for the purposes of such information broker or data collector is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

Encryption/Redaction

Georgia's data breach notification statute does not apply to personal information that is encrypted such that it is not readable or usable.

Penalties/Private Right of Action

Private Right to Action

None.

Penalties

A violation of Georgia's data breach notification statute is considered an unfair and deceptive trade practice and can result in civil penalties.

BakerHostetler

Guam

Statute

9 Guam Code §§ 48.10 - .80

Covered Entities

An individual or entity that owns or licenses computerized data that includes personal information.

Quick Notes

- **Definition of Breach.** Unauthorized access and acquisition.
- **Notification Deadline.** Without unreasonable delay.
- **Regulatory Notice Required?** No.
- **Risk of Harm Analysis?** Yes.
- **Applies to Paper Records?** No.

Definition of Personal Information

The first name or first initial and last name in combination with and linked to any one or more of the following:

- Social Security number;
- Driver's license number or Guam identification card number issued in lieu of a driver's license; or
- Financial account number or credit card or debit card number in combination with any required security code, access code, or password that would permit access to a Guam resident's financial accounts.

Definition of Breach

The unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by a covered entity as part of a database of personal information regarding multiple individuals and that causes, or the covered entity reasonably believes has caused or will cause, identity theft or other fraud to any resident of Guam.

Individual Notice

Timing

Without unreasonable delay.

Content

None specified.

Method

- Written notice to the postal address in the records of the individual or entity;
- Telephone notice; or
- Electronic notice.

Substitute Notice

Substitute notice is permitted if the covered entity demonstrates one or more of the following:

- The cost of providing notice will exceed $10,000;
- The affected class of residents to be notified exceeds 5,000 persons; or
- The covered entity does not have sufficient contact information or consent to provide notice as described in Guam's breach notification statute.

Substitute notice shall consist of any 2 of the following:

- E-mail notice, if the covered entity has e-mail addresses for the members of the Guam resident;
- Conspicuous posting of the notice on the covered entity's website, if the covered entity maintains a website; or
- Notification to major Guam media.

Credit Monitoring

Not required.

Consumer Reporting Agency Notice

Threshold

CRA notice not required.

Timing

N/A

Regulatory Notice

Regulator

None.

Threshold

N/A

Timing

N/A

Exemptions/Exceptions

HIPAA Exemption

A covered entity that complies with the notification requirements or procedures, pursuant to the rules, regulations, procedures, or guidelines established by the covered entity's primary or functional federal regulator, shall be in compliance with Guam's breach notification statute.

GLBA Exemption

A covered entity that complies with the notification requirements or procedures, pursuant to the rules, regulations, procedures, or guidelines established by the covered entity's primary or functional federal regulator, shall be in compliance with Guam's breach notification statute.

Risk of Harm

Notification is not required if an investigation determines that identify theft or fraud has not occurred or will not occur to any Guam resident.

Good Faith/Employee Acquisition

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

Encryption/Redaction

There is no breach when the information involved in the incident was redacted or encrypted.

Redacted means the following:

- An alteration or truncation of data such that no more than the following are accessible:
  - 5 digits of a Social Security Number; or
  - The last 4 digits of a driver's license number, Guam identification card number, or financial account number.

Encrypted means the following:

- A transformation of data through the use of an algorithmic process into a form in which there is a low probability of assigning, meaning without the use of a confidential process or key; or
- Securing the information by another method that renders the data elements unreadable or unusable.

Penalties/Private Right of Action

Private Right to Action

None.

Penalties

A violation that results in injury or loss to residents of Guam may be enforced by the Office of the Attorney General of Guam. The Office of the Attorney General of Guam shall have exclusive authority to bring action and may obtain actual damages for a violation or a civil penalty, not to exceed $150,000 per breach of the security of the system or series of breaches of a similar nature that are discovered in a single investigation.

BakerHostetler

Hawaii

Statute

Haw. Rev. Stat. § 487N-1

Covered Entities

An individual or entity conducting business in Hawaii that owns or licenses personal information, or any Hawaii government agency that collects personal information for specific government purposes.

Quick Notes

- **Definition of Breach.** Unauthorized access and acquisition.
- **Notification Deadline.** Without unreasonable delay.
- **Regulatory Notice Required?** Yes, if the breach requires notification of 1,000 or more Hawaii residents.
- **Risk of Harm Analysis?** Yes.
- **Applies to Paper Records?** Yes.

Definition of Personal Information

An individual's first name or first initial and last name in combination with one or more of the following:

- Social Security number;
- Driver's license number or Hawaii identification card number; or
- Account number, credit or debit card number, access code, or password that would permit access to an individual's financial account.

Definition of Breach

Unauthorized access to and acquisition of unencrypted or unredacted records or data containing personal information where illegal use of personal information has occurred or is reasonably likely to occur and that creates a risk of harm to a person.

Individual Notice

Timing:

Without unreasonable delay.

Content

- Description of incident in general terms;
- Type of personal info subject to unauthorized access/acquisition;
- General acts of business or agency to protect personal info from further unauthorized access;
- Phone number that person may call for further info, if one exists; and
- Advice that directs person to remain vigilant by reviewing account statements and monitoring credit reports.

Method

- Written notice;
- Telephonic notice, provided that contact is made directly with the affected person; or
- Electronic notice, if the notice provided is consistent with the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001 et seq.).

Substitute Notice

Substitute notice is permitted if the covered entity demonstrates one of the following:

- The cost of providing notice would exceed $100,000;
- The number of subject persons to be notified exceeds 200,000; or
- The covered entity does not have sufficient contact information or consent to satisfy direct notice.

Substitute notice shall consist of all the following:

- E-mail notice when the covered entity has an e-mail address for the subject persons;
- Conspicuous posting of the notice on the website page of the covered entity, if one is maintained; and
- Notification to major statewide media.

Credit Monitoring

Not required.

Consumer Reporting Agency Notice

Threshold

If the breach requires notification of 1,000 or more Hawaii residents.

Timing

Without unreasonable delay.

Regulatory Notice

Regulator

Hawaii Office of Consumer Protection.

Threshold

If the breach requires notification of 1,000 or more Hawaii residents.

Timing

Without unreasonable delay.

Exemptions/Exceptions

HIPAA Exemption

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 of HIPAA, shall be deemed to be in compliance with Hawaii's data breach notification statute.

GLBA Exemption

A financial institution that is subject to the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice published in the Federal Register 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, or subject to 12 C.F.R. Part 748, and any revisions, additions, or substitutions relating to the interagency guidance, shall be deemed to be in compliance with Hawaii's data breach notification statute.

Risk of Harm

Notice is not required if illegal use of personal information has not occurred, is not reasonably likely to occur, or does not create a risk of harm to a person.

Good Faith/Employee Acquisition

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.

Encryption/Redaction

There is no breach when the information involved in the incident was secured by encryption or redaction such that it was unreadable or unusable.

Penalties/Private Right of Action

Private Right of Action

Any covered entity that violates any provision of this chapter shall be liable to the injured party in an amount equal to the sum of any actual damages sustained by the injured party as a result of the violation. The court may award reasonable attorneys' fees to the prevailing party. No such action may be brought against a government agency.

The penalties are cumulative to the remedies or penalties available under all other Hawaii laws.

Penalties

Any entity that violates any provision of Hawaii's data breach notification statute shall be subject to penalties of not more than $2,500 for each violation. The Attorney General or the Executive Director of the Office of Consumer Protection may bring an action. No such action may be brought against a government agency.

BakerHostetler

Idaho

Statute

Idaho Code § 28-51-104 - Idaho Code § 28-51-107

Covered Entities

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 an Idaho resident.

Quick Notes

- **Definition of Breach.** Unauthorized acquisition.
- **Notification Deadline.** Without unreasonable delay.
- **Regulatory Notice Required?** Yes, but only for state agencies.
- **Risk of Harm Analysis?** Yes.
- **Applies to Paper Records?** No.

Definition of Personal Information

An individual's first name or first initial and last name in combination with any one or more of the following:

- Social Security number;
- Driver's license number or Idaho identification card number; or
- Account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to the individual's financial account.

Definition of Breach

Unauthorized acquisition of unencrypted, computerized data that materially compromises the security, confidentiality, or integrity of personal information for one or more persons maintained by a covered entity.

Individual Notice

Timing

Without unreasonable delay.

Content

None specified.

Method

- Written notice to the most recent address the agency, individual, or commercial entity has in its records;
- Telephonic notice; or
- Electronic notice, if the notice provided is consistent with the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001 et seq.).

Substitute Notice

Substitute notice is permitted if the covered entity demonstrates one of the following:

- The cost of providing notice would exceed $25,000;
- The affected class of subject persons to be notified exceeds 50,000; or
- The covered entity does not have sufficient contact information.

Substitute notice shall consist of all of the following:

- E-mail notice when the covered entity has an e-mail address for the Idaho resident;
- Conspicuous posting of the notice on the covered entity's website, if the covered entity maintains one; and
- Notification to major statewide media.

Credit Monitoring

Not required.

Consumer Reporting Agency Notice

Threshold

CRA notice not required.

Timing

N/A

Regulatory Notice

Regulator

Idaho Attorney General.

Threshold

Any time a state agency becomes aware of a breach of its systems.

Timing

Within 24 hours of discovery of the breach.

Exemptions/Exceptions

HIPAA Exemption

A covered 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, guidance, or guidelines established by its primary or functional state or federal regulator, is deemed to be in compliance with Idaho's breach notification statute if the covered entity complies with the maintained procedures when a breach of the security of the system occurs.

GLBA Exemption

A covered 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 Idaho's breach notification statute if the covered entity complies with the maintained procedures when a breach of the security of the system occurs.

Risk of Harm

Notification is not required if an investigation determines that the misuse of information about an Idaho resident has not occurred or is not reasonably likely to occur.

Good Faith/Employee Acquisition

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

Encryption/Redaction

There is no breach when the information involved in the incident was secured by encryption such that it was unreadable or unusable.

Penalties/Private Right of Action

Private Right of Action

None.

Penalties

Any covered entity that intentionally fails to give provide notification in accordance with Idaho's breach notification statute shall be subject to a fine of not more than $25,000 per breach of the security of the system.

BakerHostetler

Illinois

Statute

815 Ill. Comp. Stat. 530/1 et seq.

Covered Entities

Any 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.

Quick Notes

- **Definition of Breach.** Unauthorized acquisition.
- **Notification Deadline.** Without unreasonable delay.
- **Regulatory Notice Required?** Yes, if the breach requires notification of 500 or more Illinois residents.
- **Risk of Harm Analysis?** No.
- **Applies to Paper Records?** No.

Definition of Personal Information

An individual's first name or first initial and last name in combination with any one or more of the following:

- Social Security number;
- Driver's license number or state ID card number;
- Account number or credit or debit card number, or an account number or credit card number in combination with any required code or password that would permit access to an individual's financial account;
- Medical information;
- Health insurance information;
- Biometric data; or
- E-mail address in combination with a password or security question and answer that would permit access to an online account.

Definition of Breach

Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the data collector.

Individual Notice

Timing

Without unreasonable delay and in the most expedient time possible.

Content

The notice shall, at minimum, include:

- The toll-free numbers and addresses for consumer reporting agencies; and
- The toll-free number, address, and website address for the FTC and a statement that the individual can obtain information from these sources about fraud alerts and security freezes.

Notification shall not include information concerning the number of Illinois residents affected by the breach.

If compromised data is a username or e-mail address in combination with a password or security question and answer that would permit access to an online account, notice may be provided in electronic or other form. The electronic notification must direct the Illinois resident to change their username or password and security question, or to take other steps appropriate to protect all online accounts for which the resident uses the same username or e-mail address and password or security question and answer.

Method

- Written notice; or
- Electronic notice, if the notice provided is consistent with the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001 et seq.).

Substitute Notice

Substitute notice is permitted if the covered entity demonstrates one of the following:

- The cost of providing notice would exceed $250,000;
- The affected class of Illinois residents to be notified exceeds 500,000; or
- The covered entity does not have sufficient contact information.

Substitute notice shall consist of all the following:

- E-mail notice, if the data collector has the e-mail addresses to the affected persons;
- Conspicuous posting of the notice on the covered entity's website, if the covered entity maintains one; and
- Notification to major statewide media. If the breach impacts residents in one geographic area, notification to media may be made to prominent local media in areas where affected individuals are likely to reside if such notice is reasonably calculated to give actual notice to the persons to whom notice is required.

Credit Monitoring

Not required.

Consumer Reporting Agency Notice

Threshold

If the breach requires a state agency to notify 1,000 or more Illinois residents.

Timing

Without unreasonable delay.

Regulatory Notice

Regulator

The Illinois Attorney General.

Threshold

For state agencies, if the breach requires notification of 250 or more Illinois residents.

For other covered entities, if the breach requires notification of 500 or more Illinois residents.

Timing

Without unreasonable delay.

Exemptions/Exceptions

HIPAA Exemption

A covered entity is exempt from Illinois's breach notification statute if the covered entity is subject to and in compliance with the privacy and security standards for the protection of electronic health information set by HIPAA, provided that any covered entity or business associate required to provide notification of a breach to the OCR also provides such notification to the Illinois Attorney General within 5 business days of notifying the OCR.

GLBA Exemption

None.

Risk of Harm

None.

Good Faith/Employee Acquisition

Good faith acquisition of personal information by a covered entity or that covered entity's employee or agent for a legitimate purpose of that covered entity 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.

Encryption/Redaction

There is no breach when the information involved in the incident was secured by encryption, redaction, or some other method or technology that rendered the data unreadable or unusable.

Penalties/Private Right of Action

Private Right to Action

None.

Penalties

A violation of Illinois's breach notification statute constitutes an unlawful practice under Illinois's Consumer Fraud and Deceptive Business Practices Act. The Illinois Attorney General may bring an action for injunctive relief, restitution, and civil penalties against a covered entity that violates Illinois's breach notification statute.

BakerHostetler

Indiana

Statute

Ind. Code § 24-4.9-1-1 et seq. (applicable to non-governmental entities)

Ind. Code § 4-1-11-1 et seq. (applicable to state and local agencies)

Covered Entities

Any state agency, judicial or legislative department of state government, individual, corporation, business trust, estate, trust, partnership, association, nonprofit corporation or organization, cooperative, or any other legal entity that owns or licenses computerized data that includes personal information.

Quick Notes

- **Definition of Breach.** Unauthorized acquisition.
- **Notification Deadline.** Within 45 days after the discovery of the breach.
- **Regulatory Notice Required?** Yes, if the breach requires notification of 1 or more Indiana residents.
- **Risk of Harm Analysis?** Yes.
- **Applies to Paper Records?** Yes.

Definition of Personal Information

If the covered entity is not a state or local agency:

- Social Security number;
- An individual's first name or first initial and last name in combination with one or more of the following:
  - Driver's license number;
  - State ID card number;
  - Credit card number; or
  - Financial account number or debit card number in combination with a code or password that would permit access to the person's account.
- Information collected by an adult-oriented website operator or their designee.

If the covered entity is a state or local agency:

- An individual's first name or first initial and last name in combination with one or more of the following:
  - Social Security number;
  - Driver's license number or state ID card number; and
  - Account number, credit card number, debit card number, security code, access code, or password of an individual's financial account.

Definition of Breach

Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information.

Individual Notice

Timing

Without unreasonable delay, but not more than 45 days after the discovery of the breach.

Content

None specified.

Method

If the covered entity is not a state or local agency:

- Written notice;
- Telephonic notice;
- Fax; or
- E-mail, if the covered entity has the e-mail address of the Indiana resident.

If the covered entity is a state or local agency:

- Written notice; or
- E-mail, if the individual has provided the state agency with their e-mail address.

Substitute Notice

Substitute notice is permitted if the covered entity demonstrates:

- The affected class of subject persons to be notified exceeds 500,000 Indiana residents; or
- The cost of providing notice would exceed $250,000.

Substitute notice shall consist of all of the following:

- Conspicuous posting of the notice on the covered entity's website, if the covered entity maintains one; and
- Notice to major news reporting media in the geographic area where the affected Indiana residents reside.

Credit Monitoring

Not required.

Consumer Reporting Agency Notice

Threshold

If the breach requires notification of 1,000 or more Indiana residents.

Timing

Without unreasonable delay.

Regulatory Notice

Regulator

Indiana Attorney General's Office.

Threshold

When a breach requires notification to 1 or more Indiana residents.

Timing

Within 45 days of the discovery of the breach.

Exemptions/Exceptions

HIPAA Exemption

A covered entity that maintains its own disclosure procedures as part of an information privacy, security policy, or compliance plan under HIPAA is not required to make a disclosure under the Indiana data breach notification

statute if it notifies Indiana residents without unreasonable delay and complies with its information privacy, security policy, or compliance plan.

GLBA Exemption

A covered entity that maintains its own disclosure procedures as part of an information privacy, security policy, or compliance plan under GLBA is not required to make a disclosure under the Indiana data breach notification statute if it notifies Indiana residents without unreasonable delay and complies with its information privacy, security policy, or compliance plan.

A financial institution that complies with the disclosure requirements prescribed by the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice or the Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice, as applicable, is not required to make a disclosure under the Indiana data breach notification statute.

Risk of Harm

Notification is required when the covered entity knows, should know, or should have known that the unauthorized acquisition constituting the breach has resulted in or could result in identity deception, identity theft, or fraud affecting an Indiana resident.

Good Faith/Employee Acquisition

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

Encryption/Redaction

There is no breach when the information involved in the incident was secured by encryption or by any other method that renders the data unreadable or unusable.

Penalties/Private Right of Action

Private Right to Action

None.

Penalties

A covered entity that knowingly or intentionally fails to comply with any provision of the Indiana data breach notification statute commits a deceptive act that is actionable only by the Attorney General. The Attorney General may bring an action for any or all of the following:

- An injunction;
- Civil penalty not to exceed $5,000 per deceptive act; and
- Attorney General's reasonable costs in the investigation of the deceptive act and maintaining the action.

BakerHostetler

Iowa

Statute

Iowa Code § 715C.1 - Iowa Code § 715C.2

Covered Entities

Any person, 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 computerized data that includes an Iowa consumer's personal information or maintains or otherwise possesses personal information on behalf of another person.

Quick Notes

- **Definition of Breach.** Unauthorized acquisition.
- **Notification Deadline.** Without unreasonable delay.
- **Regulatory Notice Required?** Yes, if the breach requires notification of 500 or more Iowa residents.
- **Risk of Harm Analysis?** Yes.
- **Applies to Paper Records?** Yes.

Definition of Personal Information

An individual's first name or first initial and last name in combination with any one or more of the following:

- Social Security number;
- Driver's license number or other unique identification number created or collected by a government body;
- Financial account number, credit card number, or debit card number in combination with any required expiration date, security code, access code, or password that would permit access to an individual's financial account;
- Unique electronic identifier or routing code in combination with any required security code, access code, or password that would permit access to an individual's financial account; or
- Unique biometric data, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data.

Definition of Breach

Unauthorized acquisition of personal information maintained in computerized form by a person that compromises the security, confidentiality, or integrity of the personal information.

Individual Notice

Timing

If the covered entity owns or licenses the computerized data: in the most expeditious manner and without unreasonable delay.

If the covered entity maintains the computerized data: immediately following the breach discovery.

Content

- Description of breach;
- Approximate date of breach;
- Type of personal info obtained as a result of the breach;
- Contact information for consumer reporting agencies; and
- Advice to consumer to report suspected incidents of identity theft to local law enforcement or Attorney General.

Method

- Written notice; or
- Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001 et seq.).

Substitute Notice

Substitute notice is permitted if the covered entity demonstrates one of the following:

- The cost of providing notice would exceed $250,000;
- The affected class of subject persons to be notified exceeds 350,000; or
- The covered entity does not have sufficient contact information.

Substitute notice shall consist of all of the following:

- E-mail notice when the covered entity has an e-mail address for the subject persons;
- Conspicuous posting of the notice on the covered entity's website, if the covered entity maintains one; and
- Notification to major statewide media.

Credit Monitoring

Not required.

Consumer Reporting Agency Notice

Threshold

CRA notice not required.

Timing

N/A

Regulatory Notice

Regulator

Director of the Consumer Protection Division of the Iowa Attorney General's Office.

Threshold

If the breach requires notification to 500 or more Iowa residents.

Timing

Within 5 business days after giving notice of the breach to any individual.

Exemptions/Exceptions

HIPAA Exemption

Iowa's data breach notification statute does not apply to an individual who: (1) complies with notification requirements or breach of security procedures that provide greater protection to personal information and at least as thorough disclosure requirements than that provided by Iowa's data breach notification statute pursuant to the rules, regulations, procedures, guidance, or guidelines established by the person's primary or functional federal regulator; (2) complies with a state or federal law that provides greater protection to personal information and at

least as thorough disclosure requirements for breach of security or personal information than that provided by this section; or (3) is subject to and complies with regulations promulgated under HIPAA.

GLBA Exemption

Iowa's data breach notification statute does not apply to an entity who: (1) complies with notification requirements or breach of security procedures that provide greater protection to personal information and at least as thorough disclosure requirements than that provided by this section pursuant to the rules, regulations, procedures, guidance, or guidelines established by the person's primary or functional federal regulator; (2) complies with a state or federal law that provides greater protection to personal information and at least as thorough disclosure requirements for breach of security or personal information than that provided by this section; or (3) is subject to and complies with regulations promulgated under the GLBA.

Risk of Harm

Notification is not required if, after an appropriate investigation or after consultation with the relevant federal, state, or local agencies responsible for law enforcement, it is determined that no reasonable likelihood of financial harm to the consumers whose personal information has been acquired has resulted or will result from the breach. Such a determination must be documented in writing and the documentation must be maintained for five years.

Good Faith/Employee Acquisition

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.

Encryption/Redaction

Iowa's breach notification statute does not apply to personal information that is either encrypted or redacted such that it is not readable or usable.

Penalties/Private Right of Action

Private Right to Action

None.

Penalties

A violation of Iowa's breach notification statute is considered an unfair or deceptive trade practice, and the Iowa Attorney General may seek monetary damages for a violation of the statute or an injunction ordering a party to stop violating the statute.

BakerHostetler

Kansas

Statute

Kan. Stat. § 50-7a01 et seq.

Covered Entities

Any individual or entity that owns, licenses, or maintains computerized data.

Quick Notes

- **Definition of Breach.** Unauthorized access and acquisition.
- **Notification Deadline.** Without unreasonable delay.
- **Regulatory Notice Required?** No.
- **Risk of Harm Analysis?** Yes.
- **Applies to Paper Records?** No.

Definition of Personal Information

An individual's first name or first initial and last name linked to any one or more of the following:

- Social Security number;
- Driver's license number or state ID card number; or
- Financial account number, or credit or debit account number, alone or in combination with any required code or password that would permit access to an individual's financial account.

Definition of Breach

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.

Individual Notice

Timing

If a covered entity owns or licenses computerized data that contains personal information, notification must be made in the most expedient time possible following awareness of a breach. If the individual or entity maintains personal data on behalf of the data owner or licensee, notification must be made to the data owner or licensee.

Content

None specified.

Method

- Written notice; or
- Electronic notice, if the notice provided is consistent with the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001 et seq.).

Substitute Notice

Substitute notice is permitted if the covered entity demonstrates one of the following:

- The cost of providing notice would exceed $100,000;

- The affected class of consumers exceeds 5,000; or
- The covered entity does not have sufficient contact information.

Substitute notice shall consist of all of the following:

- E-mail, if the individual or entity has an e-mail address for the affected residents;
- Conspicuous posting of the notice on website, if the covered entity maintains a website; and
- Notification to major statewide media.

Credit Monitoring

Not required.

Consumer Reporting Agency Notice

Threshold

If the breach requires notification of 1,000 or more Kansas residents.

Timing

Without unreasonable delay.

Regulatory Notice

Regulator

None.

Threshold

N/A

Timing

N/A

Exemptions/Exceptions

HIPAA Exemption

A covered 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, guidance, or guidelines established by its primary or functional state or federal regulator, is deemed to be in compliance with Kansas's breach notification statute if the covered entity complies with the maintained procedures when a breach of the security of the system occurs.

GLBA Exemption

A covered 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, guidance, or guidelines established by its primary or functional state or federal regulator, is deemed to be in compliance with Kansas's breach notification statute if the covered entity complies with the maintained procedures when a breach of the security of the system occurs.

Risk of Harm

Notification is not required if an investigation determines that the misuse of information about a Kansas resident has not occurred or is not reasonably likely to occur.

Good Faith/Employee Acquisition

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

Encryption/Redaction

There is no breach when the information involved in the incident was redacted or secured by encryption such that it was unreadable or unusable.

Penalties/Private Right of Action

Private Right to Action

None.

Penalties

The Kansas Attorney General is allowed to bring action in law or equity, except as to insurance companies where the Insurance Commissioner has authority.

BakerHostetler

Kentucky

Statute

Ky. Rev. Stat. § 365.720 et seq.

Covered Entities

Any person or business that conducts business in Kentucky.

Quick Notes

- **Definition of Breach.** Unauthorized access and acquisition.
- **Notification Deadline.** Without unreasonable delay.
- **Regulatory Notice Required?** No.
- **Risk of Harm Analysis?** Yes.
- **Applies to Paper Records?** No.

Definition of Personal Information

An individual's first name or first initial and last name in combination with one or more of the following:

- Social Security number;
- Driver's license number; or
- Account number or credit or debit card number in combination with any required security code, access code, or password permitting access to an individual's financial account.

Definition of Breach

The unauthorized acquisition of unencrypted and unredacted, computerized data that compromises the security, confidentiality, or integrity of personally identifiable information that actually causes, or leads the covered entity to reasonably believe has caused or will cause, identity theft or fraud against any Kentucky resident.

Individual Notice

Timing

If the covered entity owns or licenses of the personal data, notification must be made in the most expedient time possible and without unreasonable delay. If the covered entity maintains personal data, the covered entity must notify the data owner or licensee as soon as reasonably practicable following discovery.

Content

None specified.

Method

- Written notice; or
- Electronic notice for those consumers for whom the person has a valid e-mail address and who have agreed to receive communications electronically, if the notice provided is consistent with the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001 et seq.).

Substitute Notice

Substitute notice is permitted if the covered entity demonstrates:

- The cost of providing notice would exceed $250,000;
- The affected class of subject persons to be notified exceeds 500,000; or
- The covered entity does not have sufficient contact information.

Substitute notice shall consist of:

- E-mail notice when the covered entity has an e-mail address for the subject persons;
- Conspicuous posting of the notice on the covered entity's website, if the covered entity maintains one; and
- Notification to major statewide media.

Credit Monitoring

Not required.

Consumer Reporting Agency Notice

Threshold

If the breach requires notification of 1,000 or more Kentucky residents.

Timing

Without unreasonable delay.

Regulatory Notice

Regulator

None.

Threshold

N/A

Timing

N/A

Exemptions/Exceptions

HIPAA Exemption

The provisions of Kentucky's data breach notification statute do not apply to any covered entity that is subject to the provisions of HIPAA.

GLBA Exemption

The provisions of Kentucky's data breach notification statute do not apply to any covered entity that is subject to the provisions of the GLBA.

Risk of Harm

Notification is only required when the covered entity reasonably believes the incident has caused or will cause identity theft or fraud against any Kentucky resident.

Good Faith/Employee Acquisition

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

Encryption/Redaction

There is no breach when the information involved in the incident was secured by encryption or by any other method that renders the data unreadable or unusable.

Penalties/Private Right of Action

Private Right to Action

Pursuant to Ky. Rev. Stat. § 446.070, a person injured by the violation of any statute may recover from the offender such damages as he sustained by reason of the violation, although a penalty or forfeiture is imposed for such violation.

Penalties

Violations of Kentucky's data breach notification statute may result in civil fines and other penalties.

BakerHostetler

Louisiana

Statute

La. Rev. Stat. § 51:3071 et seq.

Covered Entities

Any individual, corporation, partnership, sole proprietorship, joint stock company, joint venture, or any other legal entity that owns, licenses, or maintains computerized data that includes personal information of a resident of Louisiana.

Quick Notes

- **Definition of Breach.** Unauthorized access and acquisition.
- **Notification Deadline.** Not later than 60 days from the discovery of the breach.
- **Regulatory Notice Required?** Yes, if the breach requires notification of 1 or more Louisiana residents.
- **Risk of Harm Analysis?** Yes.
- **Applies to Paper Records?** No.

Definition of Personal Information

Individual's first name or first initial and last name in combination with any one or more of the following:

- Social Security number;
- Driver's license number or state ID number;
- Account number or credit or debit card number in combination with any required code or password that would permit access to an individual's financial account;
- Passport number; or
- Biometric data.

Definition of Breach

A compromise of the security, confidentiality, or integrity of computerized data that results in, or is reasonably likely to result in, the unauthorized acquisition of and access to personal information.

Individual Notice

Timing

Not later than 60 days from the discovery of the breach.

Content

None specified.

Method

- Written notice; or
- Electronic notice, if notice is consistent the provisions regarding electronic records and signatures in the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001 et seq.).

Substitute Notice

Substitute notice is permitted if the covered entity demonstrates one of the following:

- The cost of providing notice would exceed $100,000;

- The affected class of persons to be notified exceeds 100,000; or
- The covered entity does not have sufficient contact information.

Substitute notice shall consist of all of the following:

- E-mail notice when the covered entity has an e-mail address for the Louisiana resident;
- Conspicuous posting of the notice on the covered entity's website, if the covered entity maintains one; and
- Notification to major statewide media.

Credit Monitoring

Not required.

Consumer Reporting Agency Notice

Threshold

No CRA notice requirement.

Timing

N/A

Regulatory Notice

Regulator

The Louisiana Attorney General's Office.

Threshold

If the breach requires notification of 1 or more Louisiana residents.

Timing

If notice to residents is required, the entity must notify the Consumer Protection Section of the Attorney General's office, including names of all Louisiana citizens affected by the breach. Notice to the Attorney General's office will be "timely" if received within 10 days of notice to residents.

Exemptions/Exceptions

HIPAA Exemption

None.

GLBA Exemption

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 shall be deemed to be in compliance with Louisiana's data breach notification statute.

Risk of Harm

Notification is not required if after a reasonable investigation, the covered entity determines that there is no reasonable likelihood of harm to Louisiana residents. The covered entity shall retain a copy of the written determination and supporting documentation for 5 years from the date of discovery of the breach.

Good Faith/Employee Acquisition

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

Encryption/Redaction

There is no breach when the information involved in the incident was secured by encryption or redaction such that the data was unreadable or unusable.

Penalties/Private Right of Action

Private Right to Action

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

Penalties

A violation of Louisiana's data breach notification statute constitutes an unfair act or practice pursuant to Louisiana's consumer protection statute.

Failure to provide timely notice to the Louisiana Attorney General is punishable by a fine up to $5,000 per violation. Each day notice is not received by the Attorney General shall be deemed a separate violation.

BakerHostetler

Maine

Statute

Me. Rev. Stat. Ann. tit. 10, § 1346 et seq.

Covered Entities

Any individual, partnership, corporation, limited liability company, trust, estate, cooperative, association or other entity, including agencies of State Government, municipalities, school administrative units, public and private colleges and universities, and information brokers that maintains computerized data that includes personal information.

Quick Notes

- **Definition of Breach.** Unauthorized acquisition.
- **Notification Deadline.** Within 30 days after the covered entity becomes aware of the breach and identifies its scope.
- **Regulatory Notice Required?** Yes, if the breach requires notification of 1 or more Maine residents.
- **Risk of Harm Analysis?** Yes.
- **Applies to Paper Records?** No.

Definition of Personal Information

An individual's first name or first initial and last name in combination with any one or more of the following data elements:

- Social Security number;
- Driver's license number or State ID card number;
- Account number or credit or debit card number, if the number can be used without additional info such as a password or PIN; or
- Account passwords, PINs, or other access codes.

Any data element listed above when not connected to the individual's first name or first initial and last name, if the information would be sufficient to permit a person to compromise the identity of the person whose information was compromised.

Definition of Breach

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.

Individual Notice

Timing

Notification must be made as expediently as possible and without unreasonable delay, but no later than 30 days after the covered entity becomes aware of the breach and identifies its scope.

Content

None specified.

Method

- Written notice; or
- Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001 et seq.).

Substitute Notice

Substitute notice is permitted if the covered entity demonstrates one of the following:

- The cost of providing notice would exceed $5,000;
- The affected class of Maine residents to be notified exceeds 1,000; or
- The covered entity does not have sufficient contact information.

Substitute notice shall consist of all of the following:

- E-mail notice when the covered entity has an e-mail address for the subject persons;
- Conspicuous posting of the notice on the covered entity's website, if the covered entity maintains one; and
- Notification to major statewide media.

Credit Monitoring

Not required.

Consumer Reporting Agency Notice

Threshold

If the breach requires notification of 1,000 or more Maine residents.

Timing

Without unreasonable delay.

Regulatory Notice

Regulator

Department of Professional and Financial Regulation, if regulated by the Department. If not, notify the Maine Attorney General.

Threshold

If the breach requires notification to at least 1 Maine resident.

Timing

Not specified.

Exemptions/Exceptions

HIPAA Exemption

A covered entity that complies with the security breach notification requirements of rules, regulations, procedures, or guidelines established pursuant to federal law is deemed to be in compliance with the requirements of Maine's data breach notification statute as long as the law, rules, regulations, or guidelines provide for notification procedures at least as protective as the notification requirements.

GLBA Exemption

A covered entity that complies with the security breach notification requirements of rules, regulations, procedures, or guidelines established pursuant to federal law is deemed to be in compliance with the requirements of Maine's data breach notification statute as long as the law, rules, regulations, or guidelines provide for notification procedures at least as protective as the notification requirements.

Risk of Harm

Notification is not required if, after conducting a good faith, reasonable, and prompt investigation, the covered entity determines that there is not a reasonable likelihood that the personal information has been or will be misused.

However, the risk of harm analysis does not apply to an information broker, which must notify residents if it finds that personal information has been or is reasonably believed to have been acquired.

Good Faith/Employee Acquisition

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

Encryption/Redaction

There is no breach when the information involved in the incident was secured by encryption, redaction, or by any other method that renders the data unreadable or unusable.

Penalties/Private Right of Action

Private Right to Action

None.

Penalties

The Maine Attorney General can bring an enforcement action for the violation of Maine's breach notification statute. Civil penalties may be assessed in an amount not more than $500 per violation, up to a maximum of $2,500 for each day that a covered entity is in violation of Maine's breach notification statute. This does not apply, however, to State Government, municipalities, school administrative units, the University of Maine System, the Maine Community College System, or Maine Maritime Academy.

BakerHostetler

Maryland

Quick Notes

- **Definition of Breach.** Unauthorized acquisition.
- **Notification Deadline.** 45 days.
- **Regulatory Notice Required?** Yes, if the breach requires notification of 1 or more Maryland residents.
- **Risk of Harm Analysis?** Yes.
- **Applies to Paper Records?** No.

Statute

Md. Code Ann., Com. Law. § 14-3501 et seq.

Covered Entities

Any business, sole proprietorship, partnership, corporation, association, or any other business entity that owns, licenses, or maintains computerized data that includes personal information of an individual residing in Maryland. Business includes any financial institution organized, chartered, licensed, or otherwise authorized under the laws of Maryland, any other state, the United States, or any other country, and the parent or subsidiary of a financial institution.

Definition of Personal Information

An individual's first name or first initial and last name in combination with any one or more of the following:

- Social Security number, taxpayer ID number, passport number, or other ID number issued by the federal government;
- Driver's license or state ID card number;
- Account number or credit/debit card number in combination with any required security/access code or password that permits access to an individual's financial account;
- Health information, including information about an individual's mental health;
- Health insurance policy or certificate number or health insurance subscriber ID number, in combination with a unique identifier used by an insurer or an employer that is self-insured, that permits access to an individuals' health information;
- Biometric data; or
- Genetic information;

A username or e-mail address in combination with a password or security question and answer that permits access to an individual's e-mail account;

Genetic information with respect to an individual, including:

- Data, regardless of its format, that results from the analysis of a biological sample of the individual or from another source that enables equivalent information to be obtained and that concerns genetic material;

- Deoxyribonucleic acids;
- Ribonucleic acids;
- Genes;
- Chromosomes;
- Alleles;
- Genomes;
- Alterations or modifications to deoxyribonucleic acids or ribonucleic acids;
- Single nucleotide polymorphisms;
- Uninterrupted data that results from the analysis of a biological sample from the individual or other sources; and
- Information extrapolated, derived, or inferred from the items above.

Definition of Breach

The unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of the personal information maintained by a covered entity.

Individual Notice

Timing

No later than 45 days from the discovery or notification of the breach.

Content

- Description of categories of information breached, including elements of personal information believed to have been breached;
- Contact information for the covered entity making the notification, including address, phone number, and toll-free phone number, if one is maintained;
- Toll-free numbers and addresses for major consumer reporting agencies; and
- Toll-free phone numbers, addresses, and website addresses for the FTC and office of the Maryland Attorney General, and a statement that an individual can get information from these sources about steps to take to prevent identity theft.

Method

- Written notice;
- E-mail, provided that the individual has expressly consented to receive electronic notice or the covered entity conducts its business primarily through Internet account transactions or the Internet;
- Telephonic notice; or
- In the case of a breach where data allowing unauthorized access to a person's e-mail account, but no other personal information, is compromised, notice may be provided electronically, directing data subjects to change their passwords or security questions or take other steps appropriate to protect the e-mail account and all other online accounts for which the data subject uses the same information. The notice may not be sent by e-mail to the same e-mail account affected by the breach.

Substitute Notice

Substitute notice is permitted if the covered entity demonstrates one of the following:

- The cost of providing notice would exceed $100,000;
- The affected class of subject persons to be notified exceeds 175,000; or
- The covered entity does not have sufficient contact information.

Substitute notice shall consist of all of the following:

- E-mail notice when the covered entity has an e-mail address for the subject persons;
- Conspicuous posting of the notice on the covered entity's website, if the covered entity maintains one; and
- Notification to major statewide media.

Credit Monitoring

Not required.

Consumer Reporting Agency Notice

Threshold

If the breach requires notification of 1,000 or more Maryland residents, consumer reporting agencies must be notified of the timing, distribution, and content of the notices.

Timing

Without unreasonable delay.

Regulatory Notice

Regulator

The Maryland Attorney General.

Threshold

If the breach requires notification to one or more Maryland residents.

Timing

Prior to giving notifications to individuals, but no later than 45 days after discovery of the breach.

Exemptions/Exceptions

HIPAA Exemption

Any covered entity that is subject to and in compliance with the privacy and security standards for the protection of electronic personal health information established under HIPAA shall be deemed to be in compliance with Maryland's breach notification statute.

GLBA Exemption

Any covered entity that is subject to and in compliance with GLBA and the Federal Interagency Guidance and Response Programs for Unauthorized Access to Personal Information are deemed to be in compliance with Maryland's breach notification statute.

Risk of Harm

Notification is required only if the covered entity reasonably determines that the incident creates a likelihood that personal information has been or will be misused. The covered entity shall maintain records that reflect its determination for 3 years.

Good Faith/Employee Acquisition

Good faith acquisition of personal information by an employee or agent of the covered entity is not a breach if the personal information is used for the lawful purposes of the covered entity, provided that the personal information is not used or subject to further unauthorized disclosure.

Encryption/Redaction

There is no breach when the information involved in the incident was secured by encryption or by any other method that renders the data unreadable or unusable.

Penalties/Private Right of Action

Private Right to Action

A violation of Maryland's breach notification statute is considered an unfair or deceptive trade practice under Maryland's Consumer Protection Act and an individual may assert a private right of action to enforce the violation.

Penalties

A violation of Maryland's breach notification statute is considered an unfair or deceptive trade practice under Maryland's Consumer Protection Act and the Attorney General may bring an enforcement action.

BakerHostetler

Massachusetts

Statute

Mass. Gen. Laws 93H § 1 et seq.

Covered Entities

An individual or entity conducting business in Massachusetts or a Massachusetts government agency that owns, licenses, maintains, or stores data that includes personal information.

Quick Notes

- **Definition of Breach.** Unauthorized acquisition or use.
- **Notification Deadline.** As soon as practicable and without unreasonable delay.
- **Regulatory Notice Required?** Yes, if the breach requires notification of 1 or more Massachusetts residents.
- **Risk of Harm Analysis?** Yes.
- **Applies to Paper Records?** Yes.

Definition of Personal Information

An individual's first name or first initial and last name in combination with one or more of the following:

- Social Security number;
- Driver's license or state-issued identification card number; or
- Financial account number or credit card number with or without any required security code, access code, personal identification number, or password that would permit access to a resident's financial account.

Definition of Breach

An unauthorized acquisition or unauthorized use of electronic data maintained by a covered entity that creates a substantial risk of identity theft or fraud against a Massachusetts resident.

Individual Notice

Timing

As soon as practicable and without unreasonable delay.

Content

- The resident's right to obtain a police report.
- How a resident may request a security freeze and the necessary information to be provided when requesting the security freeze.
- That there shall be no charge for a security freeze.
- If the person or agency that experienced a breach is owned by another person or corporation, the notice to the consumer shall include the name of the parent or affiliated corporation.
- **Notice shall <u>not</u> include:**
  - the nature of the breach.
  - the number of Massachusetts residents affected.

Method

- Written notice; or
- Electronic notice, if the notice provided is consistent with the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001 et seq.).

Substitute Notice

Substitute notice is permitted if the covered entity demonstrates one of the following:

- The cost of providing written notice will exceed $250,000;
- The affected class of Massachusetts residents to be notified exceeds 500,000 residents; or
- The covered entity does not have sufficient contact information to provide notice.

Substitute notice shall consist of all of the following:

- E-mail notice, if the person or agency has e-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 covered entity, if the covered entity maintains a website; and
- Publication or broadcast through media or medium that provides notice throughout Massachusetts.

Credit Monitoring

Required at no cost for a period of not less than 18 months for Massachusetts residents whose Social Security number was involved in the breach.

Consumer Reporting Agency Notice

Threshold

CRA notice not required.

Timing

N/A

Regulatory Notice

Regulator

The Massachusetts Attorney General and The Office of Consumer Affairs and Business Regulation.

Threshold

If the breach requires notification of 1 or more Massachusetts residents.

Timing

As soon as practicable and without unreasonable delay.

Exemptions/Exceptions

HIPAA

A covered entity who maintains procedures for responding to a breach pursuant to HIPAA is deemed to be in compliance with Massachusetts' breach notification statute if the covered entity notifies affected Massachusetts residents in accordance with HIPAA, provided further that the covered entity also notifies the Attorney General and the Director of the Office of Consumer Affairs and Business Regulation of the breach as soon as practicable and without unreasonable delay.

GLBA

A covered entity who maintains procedures for responding to a breach pursuant to GLBA is deemed to be in compliance with Massachusetts' breach notification statute if the covered entity notifies affected Massachusetts residents in accordance with the GLBA, provided further that the covered entity also notifies the Attorney General and the Director of the Office of Consumer Affairs and Business Regulation of the breach as soon as practicable and without unreasonable delay.

Risk of Harm

Notice is not required if the breach does not create a substantial risk of identity theft or fraud against a Massachusetts resident.

Good Faith/Employee Acquisition

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 unless the personal information is used in an unauthorized manner or subject to further unauthorized disclosure.

Encryption/Redaction

There is no breach when the information involved in the incident was encrypted such that it was not accessible to an unauthorized actor.

Penalties/Private Right of Action

Private Right of Action

None.

Penalties

The Attorney General may bring an unfair and deceptive trade practice action which may result in a civil penalty of not more than $5,000 for each violation and may also require the covered entity to pay the reasonable costs of investigation and litigation of such violation.

BakerHostetler

Michigan

Statute

Mich. Comp. Laws § 445.63, 72 et seq.

Covered Entities

Any individual, business entity, government agency of Michigan, or other legal entity that owns or licenses data, including personal information, of a Michigan resident.

Quick Notes

- **Definition of Breach.** Unauthorized access and acquisition.
- **Notification Deadline.** Without unreasonable delay.
- **Regulatory Notice Required?** No.
- **Risk of Harm Analysis?** Yes.
- **Applies to Paper Records?** No.

Definition of Personal Information

The first name or first initial and last name linked to one or more of the following:

- Social Security number;
- Driver's license number or state personal identification card number; or
- Demand deposit or other financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to any of the resident's financial accounts.

Definition of Breach

The unauthorized access and acquisition of data that compromises the security or confidentiality of personal information maintained by a covered entity as part of a database of personal information regarding multiple individuals.

Individual Notice

Timing

Without unreasonable delay.

Content

Individual notice shall:

- Be written in a clear and conspicuous manner and shall clearly communicate the content required;
- Describe the security breach in general terms;
- Describe the type of personal information that is the subject of the unauthorized access or use;
- If applicable, generally describe what the agency or person providing the notice has done to protect data from further security breaches;
- Include a telephone number where a notice recipient may obtain assistance or additional information; and
- Remind notice recipients of the need to remain vigilant for incidents of fraud and identity theft.

Method

- Written notice;
- Telephonic notice; or
- Written notice sent electronically to the recipient, if at least one of the following conditions is met:
  - The recipient has expressly consented to receive electronic notice;
  - The covered entity has an existing business relationship with the recipient that includes periodic e-mail communications and based on those communications, the covered entity reasonably believes that it has the recipient's current e-mail address; or
  - The covered entity conducts its business primarily through Internet account transactions or on the Internet.

Substitute Notice

Substitute notice is permitted if the covered entity demonstrates one of the following:

- The cost of providing notice would exceed $250,000;
- The affected class of subject persons to be notified exceeds 500,000 Michigan residents; or
- The covered entity does not have sufficient contact information.

Substitute notice shall consist of all of the following:

- E-mail notice when the covered entity has an e-mail address for the Michigan resident;
- Conspicuous posting of the notice on the covered entity's website, if the covered entity maintains one; and
- Notification to major statewide media, which notice shall include a telephone number or website address that a person may use to obtain additional assistance and information.

A public utility that sends monthly billing or account statements to its customers may provide notice of a security breach to its customers as provided under the statute or by providing all of the following:

- As applicable, e-mail notice in accordance with Michigan's breach notification statute;
- Notice to the media reasonably calculated to inform the utility's customers of the breach;
- Conspicuous posting of notice of the security breach on the website of the utility; and
- Written notice sent in conjunction with the billing or account statement sent to the customer at his or her postal address in the utility's records.

Credit Monitoring

Not required.

Consumer Reporting Agency Notice

Threshold

CRA notice is required if a covered entity notified 1,000 or more Michigan residents of a breach.

Timing

Without unreasonable delay.

Regulatory Notice

Regulator

None.

Threshold

N/A

Timing

N/A

Exemptions/Exceptions

HIPAA Exemption

A provider of health care, health care service plan, health insurer, or a covered entity governed by the medical privacy and security rules issued by the federal Department of Health and Human Services pursuant to HIPAA shall be deemed in compliance with Michigan's breach notification statute.

GLBA Exemption

A financial institution that is subject to and in compliance with the Federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice, issued on March 7, 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 shall be deemed to be in compliance with Michigan's breach notification statute.

Risk of Harm

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

Good Faith/Employee Acquisition

A good faith but unauthorized acquisition of personal information by an employee or other individual, where the access was related to the activities of the covered entity, is not a breach of security unless the personal information is misused or disclosed to an unauthorized person. In making this determination, a covered entity shall act with the care an ordinarily prudent covered entity in a like position would exercise under similar circumstances.

Encryption/Redaction

There is no breach when the information involved in the incident was secured by encryption such that it was unreadable or unusable.

Penalties/Private Right of Action

Private Right of Action

Michigan's breach notification statute does not include a private right of action but explicitly notes that it does not eliminate other remedies available by law.

Penalties

Any covered entity that intentionally fails to provide notification in accordance with Michigan's breach notification statute may be ordered to pay a civil fine of not more than $250 for each failure to provide notice, capped at $750,000 per security breach. These penalties do not affect the availability of civil remedies under state or federal law.

BakerHostetler

Minnesota

Statute

Minn. Stat. § 325E.61 and 325E.64

Covered Entities

Any person or business that conducts business in Minnesota and that owns or licenses data that includes personal information.

Quick Notes

- **Definition of Breach.** Unauthorized acquisition.
- **Notification Deadline.** Without unreasonable delay.
- **Regulatory Notice Required?** No.
- **Risk of Harm Analysis?** No.
- **Applies to Paper Records?** No.

Definition of Personal Information

An individual's first name or first initial and last name in combination with any one or more of the following:

- Social Security number;
- Driver's license number or state identification card number; or
- Account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Definition of Breach

An unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the covered entity.

Individual Notice

Timing

In the most expedient time possible and without unreasonable delay.

Content

None specified.

Method

- Written notice; or
- Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001 et seq.).

Substitute Notice

Substitute notice is permitted if the covered entity demonstrates one of the following:

- The cost of providing notice would exceed $250,000;
- The affected class of subject persons to be notified exceeds 500,000; or

- The covered entity does not have sufficient contact information.

Substitute notice shall consist of all of the following:

- E-mail notice when the covered entity has an e-mail address for the subject persons;
- Conspicuous posting of the notice on the covered entity's website, if the covered entity maintains one; and
- Notification to major statewide media.

Credit Monitoring

Not required.

Consumer Reporting Agency Notice

Threshold

If the breach requires notification of 500 or more Minnesota residents.

Timing

Within 48 hours of notifying individuals.

Regulatory Notice

Regulator

None.

Threshold

N/A

Timing

N/A

Exemptions/Exceptions

HIPAA Exemption

None.

GLBA Exemption

Minnesota's breach notification statute does not apply to any "financial institution" as defined by the GLBA.

Risk of Harm

None.

Good Faith/Employee Acquisition

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

Encryption/Redaction

Minnesota's breach notification statute does not apply to personal information that is either encrypted or protected by another method of technology that makes electronic data unreadable or unusable.

Penalties/Private Right of Action

Private Right to Action

Any person injured by a violation of Minnesota's breach notification statute may bring a civil action and recover damages.

Penalties

The Minnesota Attorney General is entitled to sue for and have injunctive relief against any person who is found to have violated Minnesota's breach notification statute with a civil penalty in an amount to be determined by the court, not in excess of $25,000.

BakerHostetler

Mississippi

Statute

Miss. Code § 75-24-29

Covered Entities

Any natural person, business entity, and any other legal entity who conducts business in Mississippi and who, in the ordinary course of the person's business functions, owns, licenses, or maintains the personal information of any Mississippi resident.

Quick Notes

- **Definition of Breach.** Unauthorized acquisition.
- **Notification Deadline.** Without unreasonable delay.
- **Regulatory Notice Required?** No.
- **Risk of Harm Analysis?** Yes.
- **Applies to Paper Records?** No.

Definition of Personal Information

An individual's first name or first initial and last name in combination with any one or more of the following:

- Social Security number;
- Driver's license number or state identification card number; or
- Account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Definition of Breach

An unauthorized acquisition of electronic files, media, databases, or computerized data containing personal information of any Mississippi resident.

Individual Notice

Timing

Without unreasonable delay.

Content

None specified.

Method

- Written notice;
- Telephonic notice; or
- Electronic notice, if the notice provided is consistent with the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001 et seq.).

Substitute Notice

Substitute notice is permitted if the covered entity demonstrates one of the following:

- The cost of providing notice to Mississippi residents would exceed $5,000;
- The affected class of Mississippi residents to be notified exceeds 5,000; or

- The covered entity does not have sufficient contact information.

Substitute notice shall consist of all of the following:

- E-mail notice, if the covered entity has e-mail addresses for subject persons;
- Conspicuous posting of the notice on the covered entity's website, if the covered entity maintains one; and
- Notification to major statewide media.

Credit Monitoring

Not required.

Consumer Reporting Agency Notice

Threshold

CRA notice not required.

Timing

N/A

Regulatory Notice

Regulator

None required.

Threshold

N/A

Timing

N/A

Exemptions/Exceptions

HIPAA Exemption

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

GLBA Exemption

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

Risk of Harm

Notification is not required if, after an appropriate investigation, the covered entity reasonably determines that the breach will not likely result in harm to the affected Mississippi residents.

Good Faith/Employee Acquisition

None.

Encryption/Redaction

Mississippi's breach notification statute does not apply to information that is encrypted or secured by any other method or technology that renders it unreadable or unusable.

Penalties/Private Right of Action

Private Right of Action

None.

Penalties

Failure to comply with the requirements of Mississippi's breach notification statute constitutes an unfair trade practice and violations shall be enforced by the Mississippi Attorney General.

BakerHostetler

Missouri

Statute

Mo. Rev. Stat. § 407.1500

Covered Entities

Any individual, legal, or commercial or government entity that owns or licenses personal information of residents of Missouri.

Quick Notes

- **Definition of Breach.** Unauthorized access and acquisition.
- **Notification Deadline.** Without unreasonable delay.
- **Regulatory Notice Required?** Yes, if the breach requires notification of 1,000 or more Missouri residents.
- **Risk of Harm Analysis?** Yes.
- **Applies to Paper Records?** No.

Definition of Personal Information

An individual's first name or first initial and last name in combination with any one or more of the following:

- Social Security number;
- Driver's license number or other unique identification number created or collected by a government body;
- Account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account;
- Unique electronic identifier or routing code in combination with any required security code, access code, or password that would permit access to an individual's financial account;
- Medical information (information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional); or
- Health insurance information (an individual's health insurance policy number, subscriber identification number, or any unique identifier used by a health insurer to identify the individual).

Definition of Breach

Unauthorized access to and unauthorized acquisition of personal information maintained in computerized form by a covered entity that compromises the security, confidentiality, or integrity of the personal information.

Individual Notice

Timing

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

Content

The notice shall, at minimum, include:

- A description of the incident, in general terms;
- A description of the type of personal information that was involved;
- A telephone number that the affected consumer may call for further information and assistance, if one exists;
- Contact information for consumer reporting agencies; and
- Advice that directs the affected consumer to remain vigilant by reviewing account statements and monitoring free credit reports.

Method

- Written notice;
- Telephonic notice, if such contact is made directly with the affected consumers; or
- Electronic notice for those consumers for whom the person has a valid e-mail address and who have agreed to receive communications electronically, if the notice provided is consistent with the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001 et seq.).

Substitute Notice

Substitute notice is permitted if the covered entity demonstrates one of the following:

- The cost of providing notice would exceed $100,000;
- The affected class of Missouri residents to be notified exceeds 150,000; or
- The covered entity does not have sufficient contact information.

Substitute notice shall consist of all of the following:

- E-mail notice when the covered entity has an e-mail address for the Missouri resident;
- Conspicuous posting of the notice on the covered entity's website, if the covered entity maintains one; and
- Notification to major statewide media.

Credit Monitoring

Not required.

Consumer Reporting Agency Notice

Threshold

If the breach requires notification of 1,000 or more Missouri residents.

Timing

Without unreasonable delay.

Regulatory Notice

Regulator

The Missouri Attorney General.

Threshold

If the breach requires notification of 1,000 or more Missouri residents.

Timing

Without unreasonable delay.

Exemptions/Exceptions

HIPAA Exemption

A covered 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, guidance, or guidelines established by its primary or functional state or federal regulator, is deemed to be in compliance with Missouri's breach notification statute if the covered entity notifies affected consumers in accordance with the maintained procedures when a breach occurs.

GLBA Exemption

Financial institutions are deemed to be in compliance with Missouri's breach notification statute if they are subject to and in compliance with the Federal Interagency Guidance Response Programs for Unauthorized Access to Customer Information and Customer Notice, the National Credit Union Administration regulations, or Title V of the GLBA.

Risk of Harm

Notification is not required if, after an appropriate investigation or consulting with relevant law enforcement agencies, the covered entity determines the risk of identity theft or other fraud to residents is not reasonably likely to occur. The determination shall be documented in writing and maintained for five years.

Good Faith/Employee Acquisition

Good faith acquisition of personal information by a covered entity or that covered entity's employee or agent for a legitimate purpose of that covered entity 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.

Encryption/Redaction

There is no breach when the information involved in the incident was secured by encryption, redaction, or some other method or technology that rendered the data unreadable or unusable.

Penalties/Private Right of Action

Private Right of Action

None.

Penalties

The Missouri Attorney General has exclusive authority to bring an action to obtain actual damages for a willful and knowing violation of Missouri's data breach statute and may seek a civil penalty not to exceed $150,000 per breach of the security of the system or series of breaches of a similar nature that are discovered in a single investigation.

BakerHostetler

Montana

Statute

Mont. Code § 2-6-1501 et seq., 30-14-1701 et seq., 33-19-321

Covered Entities

Any person or business that conducts business in Montana, or state agency that owns or licenses computerized data that includes personal information.

Quick Notes

- **Definition of Breach.** Unauthorized acquisition.
- **Notification Deadline.** Without unreasonable delay.
- **Regulatory Notice Required?** Yes, if the breach requires notification of 1 or more Montana residents.
- **Risk of Harm Analysis?** Yes.
- **Applies to Paper Records?** No.

Definition of Personal Information

An individual's first name or first initial and last name in combination with any one or more of the following:

- Social Security number;
- Driver's license number, state identification card number, or tribal identification card number;
- Account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account;
- Medical record information, including an individual's physical or mental condition, medical history, medical claims history, medical treatment, or information obtained from a medical professional, medical care institution, the individual, or the individual's spouse, parent, or legal guardian;
- Taxpayer identification number; and
- An identity protection personal identification number issued by IRS.

Definition of Breach

The unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the covered entity and causes, or is reasonably believed to cause, loss or injury to a resident of Montana.

Individual Notice

Timing

In the most expeditious time possible and without unreasonable delay.

Content

None specified.

Method

Notice may be provided by one of the following methods:

- Written notice;
- Telephonic notice; or
- Electronic notice for those consumers for whom the person has a valid e-mail address and who have agreed to receive communications electronically, if the notice provided is consistent with the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001 et seq.).

Substitute Notice

Substitute notice is permitted if the covered entity demonstrates one of the following:

- The cost of providing notice would exceed $250,000;
- The affected class of subject persons to be notified exceeds 500,000; or
- The covered entity does not have sufficient contact information.

Substitute notice shall consist of an e-mail notice when the covered entity has e-mail addresses for the subject persons, and one of the following:

- Conspicuous posting of the notice on the covered entity's website if the covered entity maintains one; or
- Notification to major statewide or local media.

Credit Monitoring

Not required.

Consumer Reporting Agency Notice

Threshold

If the breach requires notification of one or more Montana residents and the notification suggests, indicates, or implies to the individual that the individual may obtain a copy of the file on the individual from a consumer credit reporting agency, the covered entity must notify the consumer reporting agency as to the timing, content, and distribution of the notice to the individual.

Timing

Without unreasonable delay.

Regulatory Notice

Regulator

The Montana Attorney General's Consumer Protection Office. Insurance entities and support organizations must also notify the Montana Insurance Commissioner.

Threshold

If the breach requires notification to 1 or more Montana residents.

Timing

Concurrently with notice to individuals.

Exemptions/Exceptions

HIPAA Exemption

None.

GLBA Exemption

None.

Risk of Harm

Notification is not required if the covered entity reasonably believes the breach has not and will not cause loss or injury to a Montana resident.

Good Faith/Employee Acquisition

Good faith acquisition of personal information by an employee or agent of the covered entity is not a breach if the personal information is not used for a purpose other than the lawful purpose of the covered entity and is not subject to further unauthorized disclosure.

Encryption/Redaction

There is no breach when the information involved in the incident was secured by encryption or by any other method that renders the data unreadable or unusable.

Exception

A covered entity that maintains its own notification procedures as part of an information security policy for the treatment of personal information, which does not unreasonably delay notice, is considered to be in compliance with the notification requirements of Montana's breach notification statute if the covered entity notifies the individuals in accordance with its policies.

Penalties/Private Right of Action

Private Right of Action

None.

Penalties

A violation of Montana's breach notification statute is considered an unlawful and deceptive trade practice and may result in civil penalties.

BakerHostetler

Nebraska

Statute

Neb. Rev. Stat. § 87-801 et seq.

Covered Entities

An individual, government entity, or business entity, whether for profit or not for profit, that conducts business in Nebraska and that owns or licenses computerized data that includes personal information about a resident of Nebraska.

Quick Notes

- **Definition of Breach.** Unauthorized acquisition.
- **Notification Deadline.** Without unreasonable delay.
- **Regulatory Notice Required?** Yes, if the breach requires notification of 1 or more Nebraska residents.
- **Risk of Harm Analysis?** Yes.
- **Applies to Paper Records?** No.

Definition of Personal Information

A Nebraska resident's first name or first initial and last name in combination with any one or more of the following:

- Social Security number;
- Driver's license number or state identification card number;
- Account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to a resident's financial account;
- Unique electronic ID number or routing code in combination with any required security code, access code, or password;
- Unique biometric data, such as a fingerprint, voice print, retina or iris image, or other unique physical representation; or
- A username or e-mail address in combination with a password or security question and answer that would permit access to an online account.

Definition of Breach

An unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a covered entity.

Individual Notice

Timing

Notice shall be made as soon as possible and without unreasonable delay.

Content

None specified.

Method

- Written notice;

- Telephone notice; or
- Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001 et seq.).

Substitute Notice

Substitute notice is permitted if the covered entity demonstrates one of the following:

- The cost of providing notice would exceed $75,000;
- The affected class of subject persons to be notified exceeds 100,000; or
- The covered entity does not have sufficient contact information.

Substitute notice shall consist of all of the following:

- E-mail notice when the covered entity has an e-mail address for the subject persons;
- Conspicuous posting of the notice on the covered entity's website, if the covered entity maintains one; and
- Notification to major statewide media.

Substitute notice is also permitted if the covered entity has 10 employees or fewer and demonstrates that the cost of providing notice will exceed $10,000. In this situation, substitute notice requires all of the following:

- E-mail notice, if the covered entity has e-mail addresses for the members of the affected class of Nebraska residents;
- Notification by a paid advertisement in a local newspaper that is distributed in the geographic area in which the covered entity is located, which advertisement shall be of a sufficient size that it covers at least one-quarter of a page in the newspaper and shall be published in the newspaper at least once a week for three consecutive weeks;
- Conspicuous posting of the notice on the covered entity's website, if it maintains one; and
- Notification to major media outlets in the geographic area in which the covered entity is located.

Credit Monitoring

Not required.

Consumer Reporting Agency Notice

Threshold

No CRA notice requirement.

Timing

N/A

Regulatory Notice

Regulator

Nebraska Attorney General.

Threshold

If the breach requires notification of one or more Nebraska residents.

Timing

Not later than the time when notice is provided to the Nebraska resident.

Exemptions/Exceptions

HIPAA Exemption

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, guidance, or guidelines established by its primary or functional state or federal regulator, is deemed to be in compliance with Nebraska's data breach notification statute if the individual or commercial entity notifies affected Nebraska residents and the Attorney General in accordance with the maintained procedures in the event of a breach of the security of the system.

GLBA Exemption

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, guidance, or guidelines established by its primary or functional state or federal regulator, is deemed to be in compliance with Nebraska's data breach notification statute if the individual or commercial entity notifies affected Nebraska residents and the Attorney General in accordance with the maintained procedures in the event of a breach of the security of the system.

Risk of Harm

Notification is not required if, after a good-faith, reasonable, and prompt investigation, the covered entity determines that it is unlikely that personal information has been or will be used for an unauthorized purpose.

Good Faith/Employee Acquisition

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.

Encryption/Redaction

Nebraska's breach notification statute does not apply to information that is encrypted or secured by any other method or technology that renders it unreadable or unusable.

Penalties/Private Right of Action

Private Right of Action

None.

Penalties

A violation Nebraska's breach notification statute is considered a violation of Nebraska's Consumer Protection Act. The Nebraska Attorney General may issue subpoenas and seek and recover direct economic damages for each affected Nebraska resident injured by a violation of Nebraska's breach notification statute.

BakerHostetler

Nevada

Statute

Nev. Rev. Stat. § 603A.010 et seq., 242.183

Covered Entities

Any governmental agency or business entity that owns or licenses computerized data that includes personal information.

Quick Notes

- **Definition of Breach.** Unauthorized acquisition.
- **Notification Deadline.** Without unreasonable delay.
- **Regulatory Notice Required?** No.
- **Risk of Harm Analysis?** No.
- **Applies to Paper Records?** No.

Definition of Personal Information

An individual's first name or first initial and last name in combination with any one or more of the following:

- Social Security number;
- Driver's license number, driver authorization card number, or identification card number;
- Account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account;
- A medical identification number or a health insurance identification number; or
- A username, unique identifier, or e-mail address in combination with a password, access code, or security question and answer that would permit access to an online account.

Personal information does not include the last four digits of a Social Security number, the last four digits of a driver's license or driver authorization card number, the last four digits of an identification card number, or publicly available information that is lawfully made available to the general public from federal, state, or local governmental records.

Definition of Breach

An unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the covered entity.

Individual Notice

Timing

Without unreasonable delay.

Content

None specified.

Method

- Written notice; or
- Electronic notice, if the notice provided is consistent with the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001 et seq.).

Substitute Notice

Substitute notice is permitted if the covered entity demonstrates one of the following:

- The cost of providing notice would exceed $250,000;
- The affected class of subject persons to be notified exceeds 500,000; or
- The covered entity does not have sufficient contact information.

Substitute notice shall consist of all of the following:

- E-mail notice when the covered entity has e-mail addresses for the subject persons;
- Conspicuous posting of the notice on the covered entity's website, if the covered entity maintains one; and
- Notification to major statewide media.

Credit Monitoring

Not required.

Consumer Reporting Agency Notice

Threshold

CRA notice is required if a breach requires notification to 1,000 or more Nevada residents.

Timing

Without unreasonable delay.

Regulatory Notice

Regulator

None.

Threshold

N/A

Timing

N/A

Exemptions/Exceptions

HIPAA Exemption

N/A

GLBA Exemption

A covered entity that is subject to and complies with the privacy and security provisions of the GLBA shall be deemed to be in compliance with the notification requirements of Nevada's breach notification statute.

Risk of Harm

None.

Good Faith/Employee Acquisition

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

Encryption/Redaction

There is no breach when the information involved in the incident was secured by encryption such that it was unreadable or unusable.

Penalties/Private Right of Action

Private Right of Action

None.

Penalties

The Nevada Attorney General has authority to impose civil penalties and issue injunctions against covered entities that violate Nevada's breach notification statute.

BakerHostetler

New Hampshire

Statute

N.H. Rev. Stat. § 359-C:19 et seq.

Covered Entities

An individual or entity conducting business in New Hampshire, or a New Hampshire government agency, that owns or licenses computerized data that includes personal information.

Quick Notes

- **Definition of Breach.** Unauthorized acquisition.
- **Notification Deadline.** As soon as possible.
- **Regulatory Notice Required?** Yes, if the breach requires notification of 1 or more New Hampshire residents.
- **Risk of Harm Analysis?** Yes.
- **Applies to Paper Records?** No.

Definition of Personal Information

An individual's first name or initial and last name in combination with any one or more of the following:

- Social Security number;
- Driver's license number or other government identification number; or
- Account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Definition of Breach

An unauthorized acquisition of computerized data that compromises the security or confidentiality of personal information.

Individual Notice

Timing

The covered entity shall notify the affected individuals as soon as possible.

Content

Notice shall include, at a minimum:

- 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 breach; and
- The telephone number of the covered entity.

Method

- Written notice;
- Electronic notice, if the covered entity's primary means of communication with affected individuals is by electronic means; or
- Telephonic notice, provided that a log of each such notification is kept by the covered entity.

Substitute Notice

Substitute notice is permitted if the covered entity demonstrates one of the following:

- The cost of providing notice would exceed $5,000;
- The affected class of subject individuals to be notified exceeds 1,000; or
- The covered entity does not have sufficient contact information or consent to provide written, electronic, or telephonic notice.

Substitute notice shall consist of all of the following:

- E-mail notice when the covered entity has e-mail addresses for the affected individuals;
- Conspicuous posting of the notice on the covered entity's website, if the covered entity maintains one; and
- Notification to major statewide media.

Consumer Reporting Agency Notice

Threshold

If the breach requires notification of 1,000 or more New Hampshire residents.

Timing

Without unreasonable delay.

Regulatory Notice

Regulator

The New Hampshire Attorney General.

Threshold

If the breach requires notification of 1 or more New Hampshire residents.

Timing

None specified.

Exemptions/Exceptions

HIPAA Exemption

None.

GLBA Exemption

Any covered entity engaged in trade or commerce that is subject to federal banking or securities regulators, and that maintains procedures for breach notification pursuant to the laws, rules, regulations, guidance, or guidelines issued by such regulators, shall be deemed to be in compliance with New Hampshire's data breach notification statute if it acts in accordance with such laws, rules, regulations, guidance, or guidelines.

Risk of Harm

Notice is not required if it is determined that misuse of the information has not occurred or is not reasonably likely to occur.

Good Faith/Employee Acquisition

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

Encryption/Redaction

There is no breach when the information involved in the incident was secured by encryption such that it was unreadable or unusable.

Penalties/Private Right of Action

Private Right of Action

Any person injured by any violation of New Hampshire's data breach notification statute may bring an action for damages. 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 willful or knowing, 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 attorney's fees, as determined by the court. Injunctive relief shall be available to private individuals without bond, subject to the discretion of the court.

Penalties

A violation of New Hampshire's data breach notification statute is considered an unfair or deceptive trade practice and the Attorney General can bring an action for civil penalties.

BakerHostetler

New Jersey

Statute

N.J. Stat. § 56:8-161 et seq.

Covered Entities

Any public entity or business entity, whether for profit or not for profit, that conducts business in New Jersey and that compiles or maintains computerized records that include personal information.

Quick Notes

- **Definition of Breach.** Unauthorized access.
- **Notification Deadline.** Without unreasonable delay.
- **Regulatory Notice Required?** Yes, if the breach requires notification of 1 or more New Jersey residents.
- **Risk of Harm Analysis?** Yes.
- **Applies to Paper Records?** No.

Definition of Personal Information

An individual's first name or first initial and last name linked with any one or more of the following:

- Social Security number;
- Driver's license number or state identification card number; or
- Account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.
- Username, e-mail address, or any other account holder identifying information in combination with any password or security question and answer that would permit access to an online account.

Dissociated data that, if linked, would constitute personal information is personal information if the means to link the dissociated data were accessed in connection with access to the dissociated data.

Definition of Breach

Unauthorized access to electronic files, media, or data containing personal information that compromises the security, confidentiality, or integrity of personal information, when the 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.

Individual Notice

Timing

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

Content

None specified.

Method

- Written notice; or
- Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001 et seq.).
- If the breach involves usernames or e-mail addresses in combination with a password or security question and answer that allows access to an online account, and does not involve any other personal information, notice may be made by e-mail or other form directing the New Jersey resident to change the password and security question or answer, or to take other steps to protect the account(s) where the resident uses the same username or e-mail address and password, or security question and answer.
- A covered entity that furnishes an e-mail account cannot provide notice to a user via the same affected e-mail account, but must provide notice by another approved method or by clear and conspicuous notice delivered to the consumer online when the consumer is connected to the online account from an IP address or online location from which the covered entity knows the consumer customarily accesses the account.

Substitute Notice

Substitute notice is permitted if the covered entity demonstrates one of the following:

- The cost of providing notice would exceed $250,000;
- The affected class of subject persons to be notified exceeds 500,000; or
- The covered entity does not have sufficient contact information.

Substitute notice shall consist of all of the following:

- E-mail notice when the covered entity has an e-mail address for the subject persons;
- Conspicuous posting of the notice on the covered entity's website, if the covered entity maintains one; and
- Notification to major statewide media.

Credit Monitoring

Not required.

Consumer Reporting Agency Notice

Threshold

If the breach requires notification of 1,000 or more New Jersey residents.

Timing

Without unreasonable delay.

Regulatory Notice

Regulator

Any covered entity required to provide notice under New Jersey's breach notification statute shall report the breach and any information pertaining to the breach to the New Jersey 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.

Threshold

If the breach requires notification of 1 or more New Jersey residents.

Timing

Prior to individual notice.

Exemptions/Exceptions

HIPAA Exemption

None.

GLBA Exemption

None.

Risk of Harm

Notification is not required if the covered entity determines that misuse of the personal information is not reasonably possible. The determination must be documented in writing and retained for 5 years.

Good Faith/Employee Acquisition

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

Encryption/Redaction

New Jersey's breach notification statute does not apply to information that is encrypted or secured by any other method or technology that renders it unreadable or unusable.

Penalties/Private Right of Action

Private Right of Action

None.

Penalties

The New Jersey Attorney General has authority to enforce New Jersey's breach notification statute through civil actions and injunctive relief under New Jersey's Consumer Fraud Act, which carries penalties of up to $10,000 for the first and up to $20,000 for subsequent violations.

BakerHostetler

New Mexico

Statute

N.M. Stat. 57-12C-1 et seq.

Covered Entities

Any individual or entity that owns or licenses data that includes personal information of a New Mexico resident.

Quick Notes

- **Definition of Breach.** Unauthorized acquisition.
- **Notification Deadline.** Not later than 45 days following discovery or notification of the breach.
- **Regulatory Notice Required?** Yes, if the breach requires notification of 1,000 or more New Mexico residents.
- **Risk of Harm Analysis?** Yes.
- **Applies to Paper Records?** No.

Definition of Personal Information

An individual's first name or first initial and last name in combination with one or more of the following:

- Social Security number;
- Driver's license number;
- Government-issued identification number;
- Account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to a person's financial account; or
- Biometric data.

Definition of Breach

Unauthorized acquisition of unencrypted computerized data, or of encrypted computerized data and the confidential process or key used to decrypt the encrypted computerized data, that compromises the security, confidentiality, or integrity of personal information maintained by a person.

Individual Notice

Timing

In the most expedient time possible but not later than 45 days following discovery or notification of the breach.

Content

The notice shall, at a minimum, include:

- The name and contact information of the covered entity;
- A list of the types of personal information that are reasonably believed to have been the subject of a security breach, if known;
- The date of the security breach, the estimated date of the breach, or the range of dates within which the security breach occurred, if known;
- A general description of the security breach incident;
- The toll-free telephone numbers and addresses of the major consumer reporting agencies;

- Advice that directs the recipient to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach; and
- Advice that informs the recipient of the notification of the recipient's rights pursuant to the federal Fair Credit Reporting Act.

Method

- United States mail; or
- Electronic notification, if the notice provided is consistent with the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001 et seq.).

Substitute Notice

Substitute notice is permitted if the covered entity demonstrates one of the following:

- The cost of providing notification would exceed $100,000;
- The affected class of New Mexico residents to be notified exceeds 50,000; or
- The covered entity does not have sufficient contact information.

Substitute notice shall consist of all of the following:

- Electronic notification to the e-mail addresses of New Mexico residents for whom the covered entity has valid e-mail addresses;
- Conspicuous posting of the notice on the covered entity's website, if the covered entity maintains one;
- Written notification to the New Mexico Attorney General; and
- Written notification to major media outlets in New Mexico.

Credit Monitoring

Not required.

Consumer Reporting Agency Notice

Threshold

If the breach requires notification to 1,000 or more New Mexico residents.

Timing

In the most expedient time possible but no later than 45 days following discovery or notification of the breach.

Regulatory Notice

Regulator

The New Mexico Attorney General.

Threshold

If the breach requires notification of 1,000 or more New Mexico residents.

Timing

Not specified.

Exemptions/Exceptions

HIPAA Exemption

A covered entity is exempt from New Mexico's breach notification statute if it is subject to HIPAA.

GLBA Exemption

Covered entities are deemed to be in compliance with New Mexico's breach notification statute if they are subject to the GLBA.

Risk of Harm

Notification is not required if, after an appropriate investigation, the covered entity determines that the breach does not give rise to a significant risk of identity theft or fraud.

Good Faith/Employee Acquisition

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

Encryption/Redaction

There is no breach when the information involved in the incident was secured by encryption, redaction, or some other method or technology that rendered the data unreadable or unusable.

Penalties/Private Right of Action

Private Right of Action

None.

Penalties

When the New Mexico Attorney General has a reasonable belief that a violation of New Mexico's data breach notification statute has occurred, the Attorney General may bring an action on the behalf of individuals and in the name of the state alleging a violation of the statute and seeking an injunction or damages for actual costs or losses, including consequential financial losses.

If a court determines that a person knowingly or recklessly violated New Mexico's data breach notification statute, it may impose a civil penalty of the greater of $25,000 or, in the case of failed notification, $10 per instance of failed notification, up to a maximum of $150,000.

BakerHostetler

New York

Statute

N.Y. Gen. Bus. Law § 899-aa.

Covered Entities

Any person, business, or state entity which owns, licenses, or maintains computerized data that includes private information about a New York resident.

Quick Notes

- **Definition of Breach.** Unauthorized access or acquisition.
- **Notification Deadline.** Within 30 days of discovery of the breach.
- **Regulatory Notice Required?** Yes, if the breach requires notification of 1 or more New York residents.
- **Risk of Harm Analysis?** Yes.
- **Applies to Paper Records?** No.

Definition of Personal Information

Any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person in combination with any one or more of the following:

- Social Security number;
- Driver's license number or non-driver identification card number;
- Account number or credit or debit card number in combination with any required security code, access code, password, or other information that would permit access to an individual's financial account;
- Account number or credit or debit card number, if circumstances exist wherein such number could be used to access an individual's financial account without additional identifying information, security code, access code, or password;
- Medical information;
- Health insurance information;
- Biometric information, meaning data generated by electronic measurements of an individual's unique physical characteristics, such as a fingerprint, voice print, retina or iris image, or other unique physical representation or digital representation of biometric data, used to authenticate or ascertain the individual's identity; or
- A username or e-mail address in combination with a password or security question and answer that would permit access to an online account.

Definition of Breach

Unauthorized access to or acquisition of computerized data that compromises the security, confidentiality, or integrity of private information maintained by a business.

Individual Notice

Timing

In the most expedient time possible and without unreasonable delay.

Content

- Contact information for the person or business making the notification;
- The telephone numbers and websites of the relevant state and federal agencies that provide information regarding security breaches;
- Response and identity theft prevention and protection information;
- A description of the categories of information that were or are reasonably believed to have been accessed or acquired by a person without valid authorization, including specification of the elements of personal information and private information that were or are reasonably believed to have been so accessed or acquired.

Method

- Written notice;
- Telephone notice; or
- Electronic notice, 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.

Substitute Notice

Substitute notice is permitted if the covered entity demonstrates one of the following:

- The cost of providing notice would exceed $250,000;
- The affected class of subject persons to be notified exceeds 500,000; or
- The covered entity does not have sufficient contact information.

Substitute notice shall consist of all of the following:

- E-mail notice when the covered entity has an e-mail address for the subject persons;
- Conspicuous posting of the notice on the covered entity's website, if the covered entity maintains one; and
- Notification to major statewide media.

Credit Monitoring

Not required.

Consumer Reporting Agency Notice

Threshold

If the breach requires notification of 5,000 or more New York residents.

Timing

None.

Regulatory Notice

Regulator

The New York Attorney General, the New York Department of State, the New York Division of State Police, and the New York Department of Financial Services (if the reporting entity is a “covered entity” under 23 NYCRR 500.1).

Threshold

If the breach requires notification of one or more New York residents.

Timing

Without delay.

Exemptions/Exceptions

HIPAA Exemption

If notice of a breach is made in accordance with HIPAA, no additional notice is required, but notice still must be provided to the New York Attorney General, the Department of State, the Division of State Police, and to consumer reporting agencies.

GLBA Exemption

If notice of a breach is made in accordance with Title V of the GLBA, no additional notice is required, but notice still must be provided to the New York Attorney General, the Department of State, the Division of State Police, and to consumer reporting agencies.

Risk of Harm

New York’s breach notification statute does not require notice if the exposure of private information was an inadvertent disclosure by persons authorized to access private information, and the person or business reasonably determines such exposure will not likely result in misuse of such information, financial harm to the affected persons, or emotional harm in the case of unknown disclosure of online credentials.

Good Faith/Employee Acquisition

Good faith access to or acquisition of private 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.

Encryption/Redaction

New York’s breach notification statute does not apply to information that is encrypted such that it is unreadable or unusable.

Penalties/Private Right of Action

Private Right of Action

None.

Penalties

The Attorney General may bring action for injunctive relief, damages, and if covered entity acted knowingly or recklessly, civil penalties of the greater of $5,000 or $20 per instance of failed notification, up to $250,000.

important decision that should not be based solely upon advertisements. Before you decide, ask us to send you written information about our qualifications and experience.

BakerHostetler

North Carolina

Statute

N.C. Gen. Stat. § 75-61

Covered Entities

Any business, individual, partnership, corporation, trust, estate, cooperative, association, government, governmental subdivision or agency, or other entity that owns or licenses Personal Information of residents of North Carolina, or any business that conducts business in North Carolina that owns or licenses personal information in any form.

Quick Notes

- **Definition of Breach.** Unauthorized access and acquisition.
- **Notification Deadline.** Without unreasonable delay.
- **Regulatory Notice Required?** Yes, if the breach requires notification of 1 or more North Carolina residents.
- **Risk of Harm Analysis?** Yes.
- **Applies to Paper Records?** Yes.

Definition of Personal Information

An individual's first name or first initial and last name in combination with one or more of the following:

- Social Security number or employer taxpayer identification number;
- Driver's license, state identification card, or passport number;
- Checking account number;
- Savings account number;
- Credit or debit card number;
- Payment card personal identification (PIN) code;
- Electronic identification number, e-mail names or addresses, internet account number or Internet identification name;
- Digital signatures;
- Any other numbers or information that can be used to access a person's financial resources;
- Biometric data;
- Fingerprints;
- Passwords; or
- Parent's legal surname prior to marriage.

Definition of Breach

The 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.

Individual Notice

Timing

Without unreasonable delay.

Content

The notice shall be clear and conspicuous and include all of the following:

- A description of the incident in general terms;
- A description of the type of personal information involved;
- A description of the general acts of the covered entity to protect the information from further unauthorized access;
- A telephone number for the entity that affected individuals can call for further information and assistance, if one exists;
- Advice directing the individual to stay vigilant by reviewing account statements and monitoring free credit reports;
- Toll-free number and address for the major credit reporting agencies;
- Toll-free number, address, and website address for the FTC and the Attorney General's Office; and
- A statement that the person can obtain information from these sources about identify theft.

Method

- Written notice;
- Electronic notice for those consumers for whom the person has a valid e-mail address and who have agreed to receive communications electronically, if the notice provided is consistent with the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001 et seq.); or
- Telephonic notice, provided that contact is made directly with the affected persons.

Substitute Notice

Substitute notice is permitted if the covered entity demonstrates one of the following:

- The cost of providing notice would exceed $250,000;
- The affected class of subject persons to be notified exceeds 500,000;
- The covered entity does not have sufficient contact information or consent to satisfy the notification requirements of North Carolina's breach notification law; or
- The covered entity is unable to identify particular affected individuals.

Substitute notice shall consist of all the following:

- E-mail notice when the covered entity has an e-mail address for the subject persons;
- Conspicuous posting of the notice on the covered entity's website; if the covered entity maintains one; and
- Notification to major statewide media.

Credit Monitoring

Not required.

Consumer Reporting Agency Notice

Threshold

If the breach requires notification of 1,000 or more North Carolina residents.

Timing

Without unreasonable delay.

Regulatory Notice

Regulator

The Consumer Protection Division of the Attorney General's Office.

Threshold

When a breach requires notification to 1 or more North Carolina residents.

Timing

Without unreasonable delay.

Exemptions/Exceptions

HIPAA Exemption

None.

GLBA Exemption

A financial institution that is subject to and in compliance with the notification requirements prescribed by the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, or a credit union that is subject to and in compliance with the Final Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice issued by the National Credit Union Administration, and any revisions, additions, or substitutions relating to any of the said interagency guidance shall be deemed to be in compliance with North Carolina's data breach notification statute.

Risk of Harm

Notification is not required if a breach does not result in illegal use of personal information, is not reasonably likely to result in illegal use, or there is no material risk of harm to a consumer.

Good Faith/Employee Acquisition

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.

Encryption/Redaction

North Carolina's data breach notification statute does not apply to information that is encrypted or secured by any other method or technology that renders it unreadable or unusable.

Penalties/Private Right of Action

Private Right of Action

An individual may file a lawsuit for a violation of North Carolina's data breach notification statute if the individual is injured as a result of the violation.

Penalties

A violation of North Carolina's data breach notification statute is a violation of the North Carolina Unfair or Deceptive Acts or Practices Act and may result in civil penalties.

BakerHostetler

North Dakota

Statute

N.D. Cent. Code § 51-30-01, et seq.

Covered Entities

Any person or entity conducting business in North Dakota that owns, licenses, or maintains computerized personal information.

Quick Notes

- **Definition of Breach**. Unauthorized acquisition.
- **Notification Deadline.** In the most expedient time possible and without unreasonable delay.
- **Regulatory Notice Required?** Yes, if the breach requires notification of 250 or more North Dakota residents.
- **Risk of Harm Analysis?** No.
- **Applies to Paper Records?** No.

Definition of Personal Information

An individual's first name or first initial and last name in combination with one or more of the following:

- Social Security number;
- Driver's license number;
- Nondriver color photo identification card number;
- Financial institution account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to the individual's financial accounts;
- Date of birth;
- Maiden name of the individual's mother;
- Medical information;
- Health insurance information;
- Identification number assigned to the individual by the individual's employer in combination with any required security code, access code, or password; or
- The individual's digitized or other electronic signature.

Definition of Breach

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.

Individual Notice

Timing

In the most expedient time possible and without unreasonable delay.

Content

None specified.

Method

- Written notice; or
- Electronic notice, if the notice provided is consistent with the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001 et seq.).

Substitute Notice

Substitute notice is permitted if the covered entity demonstrates one of the following:

- The cost of providing notice would exceed $250,000;
- The affected class of subject persons to be notified exceeds 500,000; or
- The covered entity does not have sufficient contact information.

Substitute notice shall consist of all of the following:

- E-mail notice when the covered entity has an e-mail address for the North Dakota resident;
- Conspicuous posting of the notice on the covered entity's website, if the covered entity maintains one; and
- Notification to major statewide media.

Credit Monitoring

Not required.

Consumer Reporting Agency Notice

Threshold

CRA notice not required.

Timing

N/A

Regulatory Notice

Regulator

The Attorney General of North Dakota.

Threshold

If the breach requires notification of 250 or more North Dakota residents.

Timing

In the most expedient time possible and without unreasonable delay.

Exemptions/Exceptions

HIPAA

A covered entity subject to the breach notification requirements under HIPAA is considered to be in compliance with North Dakota's breach notification statute.

GLBA

A financial institution 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 North Dakota's breach notification statute.

Risk of Harm

A risk of harm analysis is not permitted.

Good Faith/Employee Acquisition

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

Encryption/Redaction

There is no breach when the information involved in the incident was secured by encryption or by any other method that renders the data unreadable or unusable.

Penalties/Private Right of Action

Private Right of Action

None.

Penalties

The Attorney General may impose a civil penalty of not more than $5,000 for each violation of North Dakota's breach notification statute.

BakerHostetler

Ohio

Statute

Ohio Rev. Code Ann. § 1347.12 (state entities); Ohio Rev. Code Ann. § 1349.19 (persons and business entities)

Covered Entities

Any state agency, agency of a political subdivision, person, or business entity that conducts business in Ohio and that owns, licenses, or maintains computerized data that includes personal information.

Quick Notes

- **Definition of Breach.** Unauthorized access and acquisition.
- **Notification Deadline.** In the most expedient time possible but not later than 45 days following discovery.
- **Regulatory Notice Required?** No.
- **Risk of Harm Analysis?** Yes.
- **Applies to Paper Records?** No.

Definition of Personal Information

An individual's first name or first initial and last name in combination with and linked to any one or more of the following data elements:

- Social Security number;
- Driver's license number or state identification card number; or
- Account number or credit or debit card number in combination with and linked to any required security code, access code, or password that would permit access to an individual's financial account.

Definition of Breach

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 an Ohio resident.

Individual Notice

Timing

In the most expedient time possible but not later than 45 days following discovery or notification of the breach.

Content

None specified.

Method

- 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.

Substitute Notice

Substitute notice is permitted if the covered entity demonstrates one of the following:

- The cost of providing notice to Ohio residents would exceed $250,000;
- The affected class of Ohio residents to be notified exceeds 500,000; or
- The covered entity does not have sufficient contact information.

Substitute notice shall consist of all of the following:

- E-mail notice when the covered entity has an e-mail address for the subject persons;
- Conspicuous posting of the notice on the covered entity's website, if the covered entity maintains one; and
- Notification to major media outlets to the extent that the cumulative total of the readership, viewing audience, or listening audience of all of the outlets so notified equals or exceeds 75% of Ohio's population.

Substitute notice is also permitted if a covered entity has 10 employees or fewer, and if the cost of notification to Ohio residents will exceed $10,000. Substitute notice for covered entities with 10 or fewer employees must include:

- Notification by a paid advertisement in a local newspaper distributed in the covered entity's geographic area, which covers at least one-quarter of a page in the newspaper. Such notice must be published in the newspaper at least once a week for 3 consecutive weeks;
- Conspicuous posting of the disclosure or notice on the covered entity's website, if it maintains one; and
- Notification to major media outlets in the geographic area in which the covered entity is located.

Credit Monitoring

Not required.

Consumer Reporting Agency Notice

Threshold

If the breach requires notification of 1,000 or more Ohio residents.

Timing

Without unreasonable delay.

Regulatory Notice

Regulator

None.

Threshold

N/A

Timing

N/A

Exemptions/Exceptions

HIPAA Exemption

None.

GLBA Exemption

A financial institution, trust company, or credit union or any affiliate of a financial institution, trust company, or credit union that is required by federal law, including, but not limited to, any federal statute, regulation, regulatory guidance, or other regulatory action, to notify its customers of an information security breach with respect to information about those customers, and that is subject to examination by its functional government regulatory agency for compliance with the applicable federal law, is exempt from the requirements of Ohio's breach notification statute.

Risk of Harm

Notice is only required if the breach 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 an Ohio resident.

Good Faith/Employee Acquisition

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.

Encryption/Redaction

Ohio's breach notification statute does not apply to personal information that is encrypted, redacted, or altered by any method or technology in such a manner that the personal information is unreadable.

Penalties/Private Right of Action

Private Right of Action

None.

Penalties

The Ohio Attorney General has exclusive authority to bring an action under the Unfair Trade Practices and Consumer Protection Law for statutory violations.

The Ohio Attorney General has exclusive authority to bring a civil action seeking a temporary restraining order, preliminary or permanent injunction, and civil penalties against a person or agency that fails to comply with Ohio Rev. Code Ann. §§ 1347.12 and 1349.19.

Upon finding that a person or agency has failed to comply with Ohio's breach notification statute, a court shall impose the following civil penalties:

- $1,000 for each day the agency or person has intentionally or recklessly failed to comply with Ohio's breach notification statute, up to 60 days.
- $5,000 for each day AFTER 60 days and up to 90 days that the agency or person has intentionally or recklessly failed to comply with Ohio's breach notification statute.
- $10,000 for each day AFTER 90 days that the agency or person has intentionally or recklessly failed to comply with Ohio's breach notification statute.

BakerHostetler

Oklahoma

Statute

Okla. Stat. tit. 24 § 163

Covered Entities

Any individual or entity conducting business in Oklahoma, or an Oklahoma government agency, that owns or licenses computerized data that includes personal information.

Quick Notes

- **Definition of Breach.** Unauthorized access and acquisition.
- **Notification Deadline.** Without unreasonable delay.
- **Regulatory Notice Required?** Yes, if the breach requires notification of 500 or more Oklahoma residents.
- **Risk of Harm Analysis?** Yes.
- **Applies to Paper Records?** No.

Definition of Personal Information

An individual's first name or first initial and last name in combination with any one or more of the following:

- Social Security number;
- Driver's license number or other unique identification number created or collected by a government entity;
- Financial account number or credit card or debit card number in combination with any required expiration date, security code, access code, or password that would permit access to an individual's financial account;
- Unique electronic identifier or routing code in combination with any required security code, access code, or password that would permit access to an individual's financial account; or
- Unique biometric data such as a fingerprint, retina or iris image, or other unique physical or digital representation of biometric data to authenticate a specific individual.

Definition of Breach

Unauthorized access and acquisition of unencrypted and unredacted, computerized data that compromises the security or confidentiality of personal information maintained by a covered entity and that causes, or the covered entity reasonably believes has caused or will cause, identity theft or other fraud to any Oklahoma resident.

Individual Notice

Timing

Without unreasonable delay.

Content

None specified.

Method

- Written notice to the postal address in the records of the covered entity;
- Telephone notice; or
- Electronic notice.

Substitute Notice

Substitute notice is permitted if the covered entity demonstrates one of the following:

- The cost of providing notice will exceed $50,000;
- The affected class of residents to be notified exceeds 100,000 persons; or
- The covered entity does not have sufficient contact information or consent to provide direct notice.

Substitute notice shall consist of all of the following:

- E-mail notice, if the covered entity has e-mail addresses for the members of the affected class of residents;
- Conspicuous posting of the notice on the website of the covered entity, if the covered entity maintains a public website; and
- Notice to major statewide media.

Credit Monitoring

Not required.

Consumer Reporting Agency Notice

Threshold

CRA notice not required.

Timing

N/A

Regulatory Notice

Regulator

The Oklahoma Attorney General.

Threshold

If the breach requires notification of 500 or more Oklahoma residents.

If the breach occured at a credit bureau, notice to the Attorney General is only required if the breach impacted 1,000 or more Oklahoma residents.

Timing

Without unreasonable delay but in no event more 60 days after providing notice to impacted Oklahoma residents.

Exemptions/Exceptions

HIPAA Exemption

An entity that complies with the notification requirements or procedures pursuant to HIPAA shall be deemed to be in compliance with Oklahoma's data breach notification statute.

GLBA Exemption

A financial institution that complies with the notification requirements prescribed by the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice is deemed to be in compliance with Oklahoma's data breach notification statute.

Risk of Harm

Notice is not required if the breach will not cause identity theft or other fraud to any Oklahoma resident.

Good Faith/Employee Acquisition

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

Encryption/Redaction

There is no breach when the information involved in the incident is encrypted or redacted such that it was unreadable or unusable.

Penalties/Private Right of Action

Private Right of Action

No private right of action.

Penalties

The Attorney General or a district attorney may bring an action as an unlawful trade practice under the Oklahoma Consumer Protection Act or obtain a civil penalty not to exceed $150,000 per breach or series of breaches of a similar nature that are determined in a single investigation. Civil penalties shall be based upon the magnitude of the breach, the extent to which the behavior of the individual or entity contributed to the breach, and any failure to provide the notice required.

An individual or entity that uses reasonable safeguards and provides notice as required by Oklahoma's data breach notification statute shall not be subject to civil penalties and may use such compliance as an affirmative defense in a civil action filed under the Security Breach Notification Act.

An individual or entity that fails to use reasonable safeguards but provides notice as required by Oklahoma's data breach notification statute shall not be subject to the civil penalty set forth in subsection B of this section but shall be subject to actual damages and a civil penalty of $75,000.

BakerHostetler

Oregon

Quick Notes

- **Definition of Breach.** Unauthorized acquisition.
- **Notification Deadline.** 45 days after discovering or receiving notification of the breach.
- **Regulatory Notice Required?** Yes, if the breach requires notification to 250 or more Oregon residents.
- **Risk of Harm Analysis?** Yes.
- **Applies to Paper Records?** No.

Statute

Or. Rev. Stat. § 646A.600

Covered Entities

Any individual, private or public corporation, partnership, cooperative, association, estate, limited liability company, organization, or other entity, whether or not organized to operate at a profit, or a public body that owns, licenses, maintains, stores, manages, collects, processes, acquires, or otherwise possesses personal information in the course of the person's business.

Definition of Personal Information

An individual's first name or first initial and last name in combination with any one or more of the following:

- Social Security number;
- Driver license number or state identification card number issued by the Department of Transportation;
- Passport number or other identification number issued by the United States;
- Financial account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to a consumer's financial account, or any other information or combination of information that a person reasonably knows or should know would permit access to the consumer's financial account;
- Data from automatic measurements of a consumer's physical characteristics, such as an image of a fingerprint or retina or iris, used to authenticate the consumer's identity in the course of a financial transaction or other transaction;
- Health insurance policy number or health insurance subscriber identification number in combination with any other unique identifier that a health insurer uses to identify the consumer
- Any information about medical history, mental or physical condition, or a health care professional's medical diagnosis or treatment of the consumer; or
- A username or other means of identifying a consumer for the purpose of permitting access to the consumer's account,

together with any other method necessary to authenticate the username or means of identification.

Any of the data elements or any combination of the data elements described above without the consumer's username, or first name or first initial and last name, if:

- Encryption, redaction, or other methods have not rendered the data element or combination of data elements unusable; and
- The data element or combination of data elements would enable a person to commit identity theft against a consumer.

Definition of Breach

An unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information that a person maintains or possesses.

Individual Notice

Timing

In the most expeditious manner possible and without unreasonable delay, but not later than 45 days after discovering or receiving notification of the breach of security.

Content

The notice shall, at minimum, include:

- A description of the breach of security in general terms;
- The approximate date of the breach of security;
- The type of personal information that was subject to the breach of security;
- Contact information for the covered entity;
- Contact information for national consumer reporting agencies; and
- Advice to the consumer to report suspected identity theft to law enforcement, including the Oregon Attorney General and the Federal Trade Commission.

Method

- Written notice;
- Electronically, if the covered entity customarily communicates with the consumer electronically or if the notice is consistent with the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001 et seq.); or
- Telephone, if the covered entity contacts the affected consumer directly.

Substitute Notice

Substitute notice is permitted if the covered entity demonstrates one of the following:

- The cost of providing notice would exceed $250,000;
- The affected class of Oregon residents to be notified exceeds 350,000; or
- The covered entity does not have sufficient contact information.

Substitute notice shall include:

- Conspicuous posting of the notice on the covered entity's website, if the covered entity maintains one; and
- Notification to major statewide television and newspaper media.

Credit Monitoring

Not required.

Consumer Reporting Agency Notice

Threshold

If the breach requires notification of 1,000 or more Oregon residents.

Timing

Without unreasonable delay.

Regulatory Notice

Regulator

The Oregon Attorney General.

Threshold

If the breach requires notification to 250 or more Oregon residents.

Timing

In the most expeditious manner possible, without unreasonable delay, but not later than 45 days after discovering the breach.

Exemptions/Exceptions

HIPAA Exemption

A covered entity under HIPAA will be deemed to have complied with the notice requirements if it has complied completely with Section 13402(f) of the HITECH Act.

GLBA Exemption

A covered entity or vendor that complies with regulations promulgated under Title V of the GLBA is deemed to be in compliance with Oregon’s data breach notification statute.

Risk of Harm

Notification is not required if, after an appropriate investigation or after consultation with relevant law enforcement agencies, the covered entity reasonably determines that the breach is unlikely to cause harm. The covered entity must document the determination in writing and maintain the documentation for at least 5 years.

Good Faith/Employee Acquisition

An inadvertent acquisition of personal information by a person or the person’s employee or agent is not a breach of security if 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.

Encryption/Redaction

There is no breach when the information involved in the incident was secured by encryption, redaction, or some other method or technology that rendered the data unreadable or unusable.

Penalties/Private Right of Action

Private Right of Action

Oregon law provides for a private right of action for violations of Oregon’s data breach notification statute.

The Director of the Department of Consumer and Business Services may require a covered entity to pay compensation to consumers injured by the violation, upon a finding that a private civil action would be so burdensome or expensive as to be impractical.

Penalties

The Director of the Department of Consumer and Business Services may investigate and impose a penalty of not more than $1,000 per violation Oregon’s data breach notification statute, for a maximum of $500,000.

BakerHostetler

Pennsylvania

Statute

73 Pa. Stat. § 2301

Covered Entities

An individual or entity conducting business in Pennsylvania, or a Pennsylvania government agency, that maintains, stores, or manages computerized data that includes personal information.

Quick Notes

- **Definition of Breach.** Unauthorized access and acquisition.
- **Notification Deadline.** Without unreasonable delay.
- **Regulatory Notice Required?** Yes, if the breach requires notification of 500 or more Pennsylvania residents.
- **Risk of Harm Analysis?** Yes.
- **Applies to Paper Records?** No.

Definition of Personal Information

An individual's first name or first initial and last name in combination with one or more of the following:

- Social Security number;
- Driver's license number or a state identification card number issued in lieu of a driver's license;
- Financial account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account;
- Medical information;
- Health insurance information; or
- A username or e-mail address, in combination with a password or security question and answer that would permit access to an online account.

Definition of Breach

The unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of personal information maintained by the covered entity and that causes, or the covered entity reasonably believes has caused or will cause, loss or injury to any resident of Pennsylvania.

Individual Notice

Timing

Without unreasonable delay.

Content

None specified.

Method

- Written notice to the last known home address for the individual;
- Telephonic notice, if the individual can be reasonably expected to receive it and the notice is given in a clear and conspicuous manner, describes the incident in general terms, and verifies personal information

but does not require the individual to provide personal information and the individual is provided with a telephone number to call or website to visit for further information or assistance;
- E-mail notice, if a prior business relationship exists and the covered entity has a valid e-mail address for the individual; or
- Electronic notice, if the notice directs the person whose personal information has been materially compromised by the breach to promptly change their password and security question or answer, as applicable, or to take other steps appropriate to protect their online account to the extent the covered entity has sufficient contact information for the person.

Substitute Notice

Substitute notice is permitted if the covered entity demonstrates one of the following:
- The cost of providing notice would exceed $100,000;
- The affected class of subject persons to be notified exceeds 175,000; or
- The covered entity does not have sufficient contact information.

Substitute notice shall consist of all of the following:
- E-mail notice when the covered entity has an e-mail address for the subject persons;
- Conspicuous posting of the notice on the covered entity's website, if the covered entity maintains one; and
- Notification to major statewide media.

Credit Monitoring

Required at no cost for a period of not less than 12 months for Pennsylvania residents whose Social Security number, driver's license number, or bank account number was involved in the breach.

Consumer Reporting Agency Notice

Threshold

If the breach requires notification of 500 or more Pennsylvania residents.

Timing

Without unreasonable delay.

Regulatory Notice

Regulator

The Pennsylvania Attorney General.

Threshold

If the breach requires notification of 500 or more Pennsylvania residents.

Timing

Concurrently with notice to individuals.

Exemptions/Exceptions

HIPAA

Any covered entity or business associate that is subject to and in compliance with the privacy and security standards for the protection of electronic personal health information established under HIPAA and HITECH shall be deemed to be in compliance with Pennsylvania's breach notification statute.

GLBA

A financial institution that complies with the notification requirements prescribed by the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice is deemed to be in compliance with Pennsylvania's breach notification statute.

Risk of Harm

Notification is only required if the incident causes, or the covered entity reasonably believes has caused or will cause, loss or injury to any Pennsylvania resident.

Good Faith/Employee Acquisition

Good faith acquisition of personal information by an employee or agent of the covered entity is not a breach if the personal information is not used for a purpose other than the lawful purpose of the covered entity and is not subject to further unauthorized disclosure.

Encryption/Redaction

There is no breach when the information involved in the incident was secured by encryption or by any other method that renders the data unreadable or unusable.

Penalties/Private Right of Action

Private Right of Action

None.

Penalties

The Attorney General has exclusive authority to bring an action under the Unfair Trade Practices and Consumer Protection Law for violations of Pennsylvania's breach notification statute.

BakerHostetler

Puerto Rico

Statute

P.R. Laws Ann. tit. 10, § 4051 et seq.

Covered Entities

Any entity that is the owner or custodian of a database that includes personal information of citizens of Puerto Rico, or any entity that resells or provides access to digital data banks that contain personal information of citizens.

Quick Notes

- **Definition of Breach.** Unauthorized access.
- **Notification Deadline.** As expeditiously as possible.
- **Regulatory Notice Required?** Yes, if the breach requires notification to 1 or more Puerto Rico residents.
- **Risk of Harm Analysis?** No.
- **Applies to Paper Records?** No.

Definition of Personal Information

The name or first initial and last name of a person, together with any of the following:

- Social Security number;
- Driver's license number, voter's identification, or other official identification;
- Bank or financial account numbers of any type, with or without passwords or access codes that may have been assigned;
- Names of users and passwords or access codes to public or private information systems;
- Medical information protected by the HIPAA;
- Tax information; or
- Work-related evaluations.

Definition of Breach

Unauthorized access that compromises the security, confidentiality, or integrity of the covered data.

Individual Notice

Timing

As expeditiously as possible.

Content

The notice of breach of the security of the system shall be submitted in a clear and conspicuous manner and should describe the breach of the security of the system in general terms and the type of sensitive information compromised. The notification shall also include a tollfree number and an Internet site for people to use in order to obtain information or assistance.

Method

- Written notice; or
- Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001 et seq.).

Substitute Notice

Substitute notice is permitted if the covered entity demonstrates one of the following:

- The cost of providing notice would exceed $100,000;
- The affected class of subject persons to be notified exceeds 100,000; or
- The covered entity does not have sufficient contact information.

Substitute notice shall consist of the following:

- Prominent display of an announcement at the covered entity's premises, on the web page of the covered entity, if any, and in any informative flier published and sent through both postal and electronic mailing lists; and
- A communication to the media informing of the situation and providing information as to how to contact the covered entity to allow for better follow-up. When the information is of relevance to a specific professional or commercial sector, the announcement may be made through publications or programming of greater circulation oriented towards that sector.

Credit Monitoring

None required.

Consumer Reporting Agency Notice

Threshold

No CRA notice requirement.

Timing

N/A

Regulatory Notice

Regulator

Puerto Rico Department of Consumer Affairs.

Threshold

If the breach requires notification to one or more Puerto Rico residents.

Timing

Within a non-extendable term of 10 days after the violation of the system's security has been detected, the parties responsible shall inform the Puerto Rico Department of Consumer Affairs, which shall make a public announcement of the fact within 24 hours after having received the information.

Exemptions/Exceptions

HIPAA Exemption

None.

GLBA Exemption

None.

Risk of Harm

None.

Good Faith/Employee Acquisition

It is not considered a breach if data is accessed by normally authorized persons or entities, unless it is known or there is reasonable suspicion that they have violated the professional confidentiality or obtained authorization under false representation with the intention of making illegal use of the information.

Encryption/Redaction

Puerto Rico's data breach notification statute does not apply to information that is encrypted.

Penalties/Private Right of Action

Private Right of Action

Puerto Rico's data breach notification statute allows for a private right of action.

Penalties

Violations of Puerto Rico's data breach notification statute can result in fines of $500 to $5,000 for each violation.

BakerHostetler

Rhode Island

Statute

R.I. Gen. Laws § 11-49.3-1

Covered Entities

Any municipal agency, state agency, individual, sole proprietorship, partnership, association, corporation, joint venture, business, legal entity, trust, estate, cooperative, or other commercial entity that stores, owns, collects, processes, maintains, acquires, uses, or licenses data that includes personal information.

Quick Notes

- **Definition of Breach.** Unauthorized access or acquisition.
- **Notification Deadline.** No later than 45 days after confirmation of the breach for non-state or non-municipal agencies. No later than 30 days after confirmation of the breach for state or municipal agencies.
- **Regulatory Notice Required?** Yes, if the breach requires notification to 500 or more Rhode Island residents.
- **Risk of Harm Analysis?** Yes.
- **Applies to Paper Records?** Yes.

Definition of Personal Information

An individual's first name or first initial and last name in combination with any one or more of the following:

- Social Security number;
- Driver's license number, Rhode Island identification card number, or tribal identification number;
- Account number or credit or debit card number in combination with any required security code, access code, password, or personal identification number that would permit access to an individual's financial account;
- Medical or health insurance information; or
- E-mail address with any required security code, access code, or password that would permit access to an individual's personal, medical, insurance, or financial account.

Definition of Breach

Unauthorized access or acquisition of data (computerized or paper) that compromises the security, confidentiality, or integrity of personal information maintained by a covered entity.

Individual Notice

Timing

In the most expedient time possible, subject to the following:

- For state and municipal agencies, notification must be made no later than 30 calendar days after confirmation of the breach and the ability to ascertain the information required to fulfill the notice requirements contained in Rhode Island's breach notification statute.
- For non-state or non-municipal agencies, notification must be made no later than 45 calendar days after confirmation of the breach and the ability to ascertain the information required to fulfill the notice requirements contained in Rhode Island's breach notification statute.

Content

- A general and brief description of the incident, including how the security breach occurred and the number of affected individuals;
- The type of information that was subject to the breach;
- Date of breach, estimated date of breach, or the date range within which the breach occurred;
- Date that the breach was discovered;
- A clear and concise description of any remediation services offered to affected individuals, including toll free numbers and websites to contact the credit reporting agencies, remediation service providers, and Attorney General; and
- A clear and concise description of the consumer's ability to file or obtain a police report, how a consumer requests a security freeze and the necessary information to be provided when requesting the security freeze, and how fees may be required to be paid to the consumer reporting agencies.

Method

- Written notice; or
- Electronic notice, if the notice provided is consistent with the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001 et seq.).

Substitute Notice

Substitute notice is permitted if the covered entity demonstrates one of the following:

- The cost of providing notice to Rhode Island residents would exceed $25,000;
- The affected class of Rhode Island residents to be notified exceeds 50,000; or
- The covered entity does not have sufficient contact information.

Substitute notice shall consist of all of the following:

- E-mail notice when the municipal agency, state agency, or person has an e-mail address for the subject persons;
- Conspicuous posting of the notice on the municipal agency's, state agency's, or person's website, if the municipal agency, state agency, or person maintains one; and
- Notification to major statewide media.

Credit Monitoring

Not required.

Consumer Reporting Agency Notice

Threshold

CRA notice not required.

Timing

N/A

Regulatory Notice

Regulator

Rhode Island Attorney General.

Threshold

When a breach requires notification to 500 or more Rhode Island residents.

Timing

In the most expedient time possible, subject to the following:

- For state and municipal agencies, no later than 30 calendar days after confirmation of the breach and the ability to ascertain the information required to fulfill the notice requirements contained in Rhode Island's breach notification statute.

- For non-state or non-municipal agencies, no later than 45 calendar days after confirmation of the breach and the ability to ascertain the information required to fulfill the notice requirements contained in Rhode Island's breach notification statute.

Exemptions/Exceptions

HIPAA Exemption

A provider of health care, healthcare service plan, health insurer, or a covered entity governed by HIPAA shall be deemed in compliance with Rhode Island's breach notification statute..

GLBA Exemption

A financial institution, trust company, credit union, or its affiliates that is subject to and examined for, and found in compliance with, the Federal Interagency Guidelines on Response Programs for Unauthorized Access to Customer Information and Customer Notice shall be deemed in compliance with Rhode Island's breach notification statute.

A covered entity shall be deemed to be in compliance with Rhode Island's breach notification statute if it maintains a security breach procedure pursuant to the rules, regulations, procedures, or guidelines established by the primary or functional regulator, as defined in 15 U.S.C. § 6809(2), and notifies subject persons in accordance with the policies or the rules, regulations, procedures, or guidelines established by the primary or functional regulator in the event of a breach of security of the system.

Risk of Harm

Notification is not required if an investigation determines a breach does not pose a "significant risk of identity theft" to a Rhode Island resident.

Good Faith/Employee Acquisition

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

Encryption/Redaction

Rhode Island's breach notification statute does not apply to personal information that is encrypted in such a manner that the personal information is unreadable.

Penalties/Private Right of Action

Private Right of Action

None.

Penalties

The Rhode Island Attorney General may bring action and seek civil penalties up to $100 per occurrence for a violation of Rhode Island's breach notification statute, or $200 per occurrence for a knowing and willful violation of Rhode Island's breach notification statute.

BakerHostetler

South Carolina

Statute

S.C. Code § 39-1-90

Covered Entities

An individual or entity conducting business in South Carolina that owns or licenses computerized data or other data that includes personal information.

Quick Notes

- **Definition of Breach.** Unauthorized access and acquisition.
- **Notification Deadline.** Without unreasonable delay.
- **Regulatory Notice Required?** Yes, if the breach requires notification of 1,000 or more South Carolina residents.
- **Risk of Harm Analysis?** Yes.
- **Applies to Paper Records?** Yes.

Definition of Personal Information

The first name or first initial and last name in combination with and linked to any one or more of the following:

- Social Security number;
- Driver's license number or state identification card number issued in lieu of a driver's license;
- Financial account number or credit card or debit card number in combination with any required security code, access code, or password that would permit access to a resident's financial account; or
- Other numbers or information which may be used to access a person's financial accounts, or numbers or information issued by a governmental or regulatory entity that uniquely will identify an individual.

Definition of Breach

Unauthorized access to and acquisition of computerized data when illegal use of the information has occurred or is reasonably likely to occur, or use of the information creates a material risk of harm to a South Carolina resident.

Individual Notice

Timing

In the most expedient time possible and without unreasonable delay.

Content

None specified.

Method

- Written notice;
- Electronic notice, if the notice provided is consistent with the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001 et seq.); or
- Telephonic notice.

Substitute Notice

Substitute notice is permitted if the covered entity demonstrates one of the following:

- The cost of providing notice exceeds $250,000;
- The affected class of subject persons to be notified exceeds 500,000; or
- The covered entity has insufficient contact information.

Substitute notice shall consist of all of the following:

- E-mail notice when the covered entity has an e-mail address for the subject persons;
- Conspicuous posting of the notice on the website page of the covered entity, if the covered entity maintains one; and
- Notification to major statewide media.

Credit Monitoring

Not required.

Consumer Reporting Agency Notice

Threshold

If the breach requires notification of 1,000 or more South Carolina residents.

Timing

Without unreasonable delay.

Regulatory Notice

Regulator

The Consumer Protection Division of the Department of Consumer Affairs.

Threshold

If the breach requires notification of 1,000 or more South Carolina residents.

Timing

In the most expedient time possible and without unreasonable delay.

Exemptions/Exceptions

HIPAA Exemption

None.

GLBA Exemption

South Carolina's data breach notification statute does not apply to a bank or financial institution that is subject to and in compliance with the privacy and security provision of GLBA. A financial institution that is subject to and in compliance with the Federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice, issued March 7, 2005, as amended, 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 is considered to be in compliance with South Carolina's data breach notification statute.

Risk of Harm

Notice is not required if illegal use of the information has not occurred, is not reasonably likely to occur, or use of the information does not create a material risk of harm to the South Carolina resident.

Good Faith/Employee Acquisition

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

Encryption/Redaction

There is no breach when the information involved in the incident was secured by encryption such that it was unreadable or unusable.

Penalties/Private Right of Action

Private Right of Action

A South Carolina resident who is injured by a violation of South Carolina's data breach notification statute may bring a civil action, in addition to and cumulative of all other rights and remedies available at law.

Penalties

A covered entity who knowingly and willfully violates South Carolina's data breach notification statute is subject to an administrative fine in the amount of $1,000 for each resident whose information was accessible because of the breach.

BakerHostetler

South Dakota

Statute

S.D. Code 22-40-20 et seq.

Covered Entities

Any person or business that conducts business in the state and that owns or licenses computerized personal or protected information of South Dakota residents.

Quick Notes

- **Definition of Breach.** Unauthorized access and acquisition.
- **Notification Deadline.** No later than 60 days after confirmation of the breach.
- **Regulatory Notice Required?** Yes, if the breach requires notification to 250 or more South Dakota residents.
- **Risk of Harm Analysis?** Yes.
- **Applies to Paper Records?** No.

Definition of Personal Information

An individual's first name or first initial and last name in combination with any one or more of the following:

- Social Security number;
- Driver's license number or other unique identification number created or collected by a government body;
- Account, credit card, or debit card number in combination with any required security code, access code, password, routing number, PIN, or any additional information that would permit access to a person's financial account;
- Health information as defined in 45 CFR 160.103;
- An identification number assigned to a person by the person's employer in combination with any required security code, access code, password, or biometric data generated from measurements or analysis of human body characteristics for authentication purposes;
- A username or e-mail address in combination with a password, security question and answer, or other information that permits access to an online account; or
- An account number or credit or debit card number in combination with any required security code, access code, or password that permits access to a person's financial account.

Definition of Breach

The unauthorized acquisition of unencrypted, computerized data, or encrypted, computerized data and the encryption key, by any person that materially compromises the security, confidentiality, or integrity of personal or protected information maintained by the covered entity.

Individual Notice

Timing

Not later than 60 days from the date a covered entity discovers a breach or is notified of a breach.

Content

None specified.

Method

- Written notice; or
- Electronic notice, if the notice provided is consistent with the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001 et seq.), or if the covered entity's primary method of communication with the residents of this state has been by electronic means.

Substitute Notice

Substitute notice is permitted if the covered entity demonstrates one of the following:

- The covered entity demonstrates that the cost of providing notice would exceed $250,000;
- The affected class of persons to be notified exceeds 500,000 persons; or
- The covered entity does not have sufficient contact information.

Substitute notice shall consist of all of the following:

- E-mail notice, if the covered entity has e-mail addresses for the South Dakota residents;
- Conspicuous posting of the notice on the covered entity's website, if the covered entity maintains a website page; and
- Notification to statewide media.

Credit Monitoring

Not required.

Consumer Reporting Agency Notice

Threshold

CRA notice is required if a breach requires notification to one or more South Dakota residents.

Timing

None specified.

Regulatory Notice

Regulator

South Dakota Attorney General.

Threshold

If a breach requires notification to 250 or more South Dakota residents.

Timing

None specified.

Exemptions/Exceptions

HIPAA Exemption

A covered entity that is regulated by federal law or regulation 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 federal regulator, is deemed to be in compliance with South Dakota's breach notification statute if the covered entity notifies affected South Dakota residents in accordance with the provisions of the applicable federal law or regulation when a breach of the security of the system occurs.

GLBA Exemption

A covered entity that is regulated by federal law or regulation 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 federal regulator, is deemed to be in compliance with South Dakota's breach notification statute if the covered entity notifies affected South Dakota residents in accordance with the provisions of the applicable federal law or regulation when a breach of the security of the system occurs.

Risk of Harm

Notification is not required if an investigation determines that the breach will not likely result in harm to South Dakota residents or that the unauthorized acquisition does not materially compromise the security, confidentiality, or integrity of personal information.

Good Faith/Employee Acquisition

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

Encryption/Redaction

There is no breach when the information involved in the incident was secured by encryption such that it was unreadable or unusable.

Penalties/Private Right of Action

Private Right of Action

None.

Penalties

The South Dakota Attorney General may prosecute each failure to disclose under South Dakota's breach notification statute as a deceptive act or practice. In addition, the South Dakota Attorney General may bring an action to recover a civil penalty on behalf of the state of not more than $10,000 per day per violation of South Dakota's breach notification statute. The South Dakota Attorney General may recover attorney's fees and any costs associated with any action brought under South Dakota's breach notification statute.

BakerHostetler

Tennessee

Statute

Tenn. Code § 47-18-2107.

Covered Entities

Any natural person, consumer, individual, business, governmental agency, partnership, corporation, trust, estate, incorporated or unincorporated association, and any other legal or commercial entity, however organized, that conducts business in Tennessee, or any Tennessee agency or any of its political subdivisions, that owns or licenses computerized data that includes personal information of Tennessee residents or maintains computerized data that includes personal information that the information holder does not own.

Quick Notes

- **Definition of Breach.** Unauthorized acquisition.
- **Notification Deadline.** 45 days from the discovery or notification of the breach.
- **Regulatory Notice Required?** Yes, but only for state agencies.
- **Risk of Harm Analysis?** Yes.
- **Applies to Paper Records?** No.

Definition of Personal Information

An individual's first name or first initial and last name in combination with any one or more of the following:

- Social Security number;
- Driver's license number;
- Account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Definition of Breach

Acquisition of information (either unencrypted, computerized data or encrypted, computerized data and the encryption key) by an unauthorized person that materially compromises the security, confidentiality, or integrity of personal information maintained by the covered entity.

Individual Notice

Timing

Immediately, but no later than 45 days following discovery or notification of the breach.

Content

None specified.

Method

- Written notice; or
- Electronic notice, if the notice provided is consistent with the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001 et seq.).

Substitute Notice

Substitute notice is permitted if the covered entity demonstrates one of the following:

- The cost of providing notice would exceed $250,000;

- The affected class of Tennessee residents to be notified exceeds 500,000; or
- The covered entity does not have sufficient contact information.

Substitute notice shall consist of all of the following:

- E-mail notice when the covered entity has an e-mail address for the subject persons;
- Conspicuous posting of the notice on the covered entity's website, if the covered entity maintains one; and
- Notification to major statewide media.

Credit Monitoring

Not required.

Consumer Reporting Agency Notice

Threshold

If the breach requires notification of 1,000 or more Tennessee residents.

Timing

Without unreasonable delay.

Regulatory Notice

Regulator

State agencies must notify the Comptroller of the Treasury of any confirmed or suspected unauthorized acquisition of computerized data and any confirmed or suspected breach of a computer information system or related security system established to safeguard the data and computer information system.

Threshold

None specified.

Timing

Within 5 working days after confirming or suspecting the unauthorized acquisition or breach.

Exemptions/Exceptions

HIPAA Exemption

Tennessee's breach notification statute does not apply to any covered entity that is subject to HIPAA, as expanded by the HITECH Act.

GLBA Exemption

Tennessee's breach notification statute does not apply to any covered entity that is subject to Title V of the GLBA.

Risk of Harm

Notification is only required if the unauthorized acquisition of information "materially compromises" the security, confidentiality, or integrity of personal information maintained by the covered entity.

Good Faith/Employee Acquisition

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

Encryption/Redaction

Tennessee's breach notification statute does not apply to information that is encrypted or secured by any other method or technology that renders it unreadable or unusable.

Penalties/Private Right of Action

Private Right of Action

Any customer of a covered entity who is a person or business entity, but who is not a Tennessee agency or any Tennessee political subdivision, and who is injured by a violation of Tennessee's breach notification statute, may institute a civil action to recover damages and to enjoin the covered entity from further action in violation of the statute.

Penalties

A violation of Tennessee's breach notification statute constitutes a violation of the Tennessee Consumer Protection Act. If the Tennessee Attorney General has reason to believe that a covered entity has violated Tennessee's breach notification statute, then the Tennessee Attorney General may institute an enforcement proceeding to seek civil penalties.

BakerHostetler

Texas

Statute

Tex. Bus. & Com. Code § 521.002, Tex. Bus. & Com. Code § 521.053

Covered Entities

An entity who conducts business in the state and owns or licenses computerized data that includes personal information, or any person who maintains computerized data that includes sensitive personal information not owned by the person.

Quick Notes

- **Definition of Breach.** Unauthorized acquisition.
- **Notification Deadline.** Within 60 days after learning that the breach occurred.
- **Regulatory Notice Required?** Yes, if the breach requires notification of 250 or more Texas residents.
- **Risk of Harm Analysis?** No.
- **Applies to Paper Records?** No.

Definition of Personal Information

An individual's first name or first initial and last name in combination with any one or more of the following:

- Social Security number;
- Driver's license number or government-issued identification number; or
- Account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; or
- Information that identifies an individual and relates to:
  - The physical or mental health or condition of the individual;
  - The provision of healthcare to the individual; or
  - The payment for the provision of healthcare to the individual.

Definition of Breach

The unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information, excluding certain good faith acquisitions.

Individual Notice

Timing

Without unreasonable delay, but no later than 60 days after discovery of the breach, consistent with measures necessary to determine the scope of the breach and restore the reasonable integrity of the system.

Content

None specified.

Method

- Written notice; or
- Electronic notice for those consumers for whom the person has valid e-mail addresses and who have agreed to receive communications electronically, if the notice provided is consistent with the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001 et seq.).

Substitute Notice

Substitute notice is permitted if the covered entity demonstrates one of the following:

- The cost of providing notice would exceed $250,000;
- The affected class of subject persons to be notified exceeds 500,000; or
- The covered entity does not have sufficient contact information.

Substitute notice may consist of any of the following:

- E-mail notice when the covered entity has an e-mail address for the subject persons;
- Conspicuous posting of the notice on the covered entity's website, if the covered entity maintains one; or
- Notification to major statewide media.

Credit Monitoring

Not Required.

Consumer Reporting Agency Notice

Threshold

If the breach requires notification of 10,000 or more Texas residents, consumer reporting agencies must be notified of the timing, distribution, and content of the notice given to the residents of the state.

Timing

Without unreasonable delay.

Regulatory Notice

Regulator

The Attorney General of Texas.

Threshold

If the breach requires notification of 250 or more Texas residents.

Timing

Without unreasonable delay, but no later than 30 days after learning that the breach occurred.

Exemptions/Exceptions

HIPAA Exemption

None.

GLBA Exemption

None.

Risk of Harm

None.

Good Faith/Employee Acquisition

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 system security unless the person uses or discloses the sensitive personal information in an unauthorized manner.

Encryption/Redaction

The unauthorized acquisition of encrypted, computerized data does not constitute a “breach of system security” so long as the encryption key was also not acquired.

Penalties/Private Right of Action

Private Right of Action

None.

Penalties

Violations of Texas’s breach notification statute are considered deceptive trade practices. The Attorney General can bring enforcement actions under the statute to recover civil penalties, obtain injunctive relief, and recover attorneys’ fees and costs. Violations may result in civil penalties, including penalties to the state between $2,000 and $50,000 per violation. Additionally, failure to comply with the notification provisions may result in civil penalties of up to $100 for each individual for whom notification is due for each day that the covered entity fails to take reasonable action to comply with such notification provisions.

BakerHostetler

U.S. Virgin Islands

Statute

V.I. Code Ann. tit. 14, §2208 - 2212

Covered Entities

Any person, business, or agency that owns, licenses, or maintains computerized data that includes personal information about a U.S. Virgin Islands resident.

Quick Notes

- **Definition of Breach.** Unauthorized acquisition.
- **Notification Deadline.** In the most expedient time possible and without unreasonable delay.
- **Regulatory Notice Required?** No.
- **Risk of Harm Analysis?** No.
- **Applies to Paper Records?** No.

Definition of Personal Information

An individual's first name or first initial and last name in combination with any one or more of the following:

- Social Security number;
- Driver's license number; or
- Account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Definition of Breach

Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the covered entity.

Individual Notice

Timing

In the most expedient time possible and without unreasonable delay.

Content

None specified.

Method

- Written notice; or
- Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001 et seq.).

Substitute Notice

Substitute notice is permitted if the covered entity demonstrates one of the following:

- The cost of providing notice would exceed $100,000;
- The affected class of subject persons to be notified exceeds 50,000; or

- The covered entity does not have sufficient contact information.

Substitute notice shall consist of all of the following:

- E-mail notice when the covered entity has an e-mail address for the subject persons;
- Conspicuous posting of the notice on the covered entity's website, if the covered entity maintains one; and
- Notification to major territory-wide media.

Credit Monitoring

None required.

Consumer Reporting Agency Notice

Threshold

No CRA notice requirement.

Timing

N/A

Regulatory Notice

Regulator

None.

Threshold

N/A

Timing

N/A

Exemptions/Exceptions

HIPAA Exemption

None.

GLBA Exemption

None.

Risk of Harm

None.

Good Faith/Employee Acquisition

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

Encryption/Redaction

The U.S. Virgin Island's breach notification statute does not apply to information that is encrypted.

Penalties/Private Right of Action

Private Right of Action

Any customer injured by a violation of the U.S. Virgin Island's breach notification statute may commence a civil action to recover damages.

Penalties

Violations of the U.S. Virgin Island's breach notification statute may result in civil penalties.

BakerHostetler

Utah

Statute

Utah Code § 13-44-101 et seq.

Covered Entities

An individual, business entity, or any unincorporated organization who owns, licenses, or maintains computerized data that includes personal information concerning a Utah resident.

Quick Notes

- **Definition of Breach.** Unauthorized acquisition.
- **Notification Deadline.** In the most expedient time possible and without unreasonable delay.
- **Regulatory Notice Required?** Yes, if the breach requires notification to 500 or more Utah residents.
- **Risk of Harm Analysis?** Yes.
- **Applies to Paper Records?** No.

Definition of Personal Information

A person's first name or first initial and last name in combination with any one or more of the following:

- Social Security number;
- Financial account number or credit or debit card number, including the required security code, access code, or password that would permit access to the person's account; or
- Driver's license number or state identification card number.

Definition of Breach

Unauthorized acquisition of computerized data maintained by a covered entity that compromises the security, confidentiality, or integrity of personal information.

Individual Notice

Timing

In the most expedient time possible and without unreasonable delay.

Content

None specified.

Method

- Written notice, by first-class mail to the most recent address the covered entity has for the resident;
- Electronic notice, if the notice provided is consistent with the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001 et seq.); or
- Telephonic notice, including through the use of automatic dialing technology not prohibited by other law.

Substitute Notice

Substitute notice is permitted if the covered entity demonstrates that written notice, electronic notice, and telephonic notice are not feasible.

Substitute notice shall consist of publishing notification of the breach in a newspaper of general circulation.

Credit Monitoring

Not required.

Consumer Reporting Agency Notice

Threshold

CRA notice is required if 1,000 or more Utah residents are notified.

Timing

Not specified.

Regulatory Notice

Regulator

The Attorney General of Utah and the Utah Cyber Center.

Threshold

If the breach requires notification to 500 or more Utah residents.

Timing

In the most expedient time possible and without unreasonable delay.

Exemptions/Exceptions

HIPAA Exemption.

A covered entity who is regulated by state or federal law and maintains procedures for a breach of system security under applicable law established by the primary state or federal regulator is considered to be in compliance with Utah's breach notification statute if the covered entity notifies each affected Utah resident in accordance with the other applicable law in the event of a breach.

GLBA Exemption

A covered entity who is regulated by state or federal law and maintains procedures for a breach of system security under applicable law established by the primary state or federal regulator is considered to be in compliance with Utah's breach notification statute if the covered entity notifies each affected Utah resident in accordance with the other applicable law in the event of a breach.

Risk of Harm

Notification is not required if an investigation determines that the misuse of information about a Utah resident has not occurred or is not reasonably likely to occur.

Good Faith/Employee Acquisition

Good faith acquisition of personal information by an employee or agent of an agency, individual, or a commercial entity for the purposes of the agency, individual, or commercial entity 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.

Encryption/Redaction

There is no breach when the information involved in the incident was secured by encryption such that it was unreadable or unusable.

Penalties/Private Right of Action

Private Right of Action

None.

Penalties

A covered entity who violates the provisions of Utah's breach notification statute is subject to a civil penalty of:

- No greater than $2,500 for a violation or series of violations concerning a specific consumer; and
- No greater than $100,000 in the aggregate for related violations concerning more than one consumer, unless the violations concern:
  - 10,000 or more consumers who are residents of the state; and
  - 10,000 or more consumers who are residents of other states; or
  - The covered entity agrees to settle for a greater amount.

In addition to civil penalties, the Utah Attorney General may seek:

- Injunctive relief to prevent future violations of Utah's breach notification statute; and
- Attorney fees and costs.

BakerHostetler

Vermont

Statute

Vt. Stat. tit. 9, § 2435 et seq.

Covered Entities

An individual or entity conducting business in Vermont, or a Vermont government agency, that owns, licenses, maintains, or possesses computerized data containing personal information.

Quick Notes

- **Definition of Breach.** Unauthorized acquisition.
- **Notification Deadline.** Within 45 days of discovery of the breach.
- **Regulatory Notice Required?** Yes, if the breach requires notification of 1 or more Vermont residents.
- **Risk of Harm Analysis?** Yes.
- **Applies to Paper Records?** No.

Definition of Personal Information

An individual's first name or first initial and last name in combination with one or more of the following:

- Social Security number;
- Driver's license or nondriver state identification card number, individual taxpayer identification number, passport number, military identification card number, or other identification number that originates from a government identification document that is commonly used to verify identity for a commercial transaction;
- Financial account number or credit or debit card number, if the number could be used without additional identifying information, access codes, or passwords;
- Password, personal identification number, or other access code for a financial account;
- Unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee of the data to identify or authenticate the individual, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data;
- Genetic information;
- Health records or records of a wellness program or similar program of health promotion or disease prevention;
- Healthcare professional's medical diagnosis or treatment of the individual;
- Health insurance policy number; or
- An individual's username or e-mail address in combination with a password

or security question and answer that together permit access to an online account.

Definition of Breach

Unauthorized acquisition of electronic data, or a reasonable belief of an unauthorized acquisition of electronic data, that compromises the security, confidentiality, or integrity of personal information maintained by a covered entity.

Individual Notice

Timing

In the most expedient time possible and without unreasonable delay, but not later than 45 days after discovery of the breach.

Content

- The incident in general terms;
- The type of personal information that was subject to the breach;
- The general acts of the covered entity to protect the personal information from further breach;
- A telephone number, toll-free if available, that the individual may call for further information and assistance;
- Advice that directs the individual to remain vigilant by reviewing account statements and monitoring free credit reports; and
- The approximate date of the breach.

Method

- Written notice mailed to the individual's residence.
- Electronic notice for those individuals for whom the covered entity has a valid e-mail address, if:
  - The covered entity's primary method of communication with the individual is by electronic means, the electronic notice does not request or contain a hypertext link to a request that the individual provide personal information, and the electronic notice conspicuously warns individuals not to provide personal information in response to electronic communications regarding security breaches; or
  - The notice is consistent with the provisions regarding electronic records and signatures for notices in the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001 et seq.).
- Telephonic notice, provided that telephonic contact is made directly with each affected individual and not through a prerecorded message.

Substitute Notice

Substitute notice is permitted if the covered entity demonstrates one of the following:

- That the lowest cost of providing direct notice would exceed $10,000; or
- The covered entity does not have sufficient contact information.

Substitute notice shall consist of all of the following:

- Conspicuously posting the notice on the covered entity's website, if the covered entity maintains one; and
- Notifying major statewide and regional media.

Credit Monitoring

Not required.

Consumer Reporting Agency Notice

Threshold

If the breach requires notification of 1,000 or more Vermont residents.

Timing

Without unreasonable delay.

Regulatory Notice

Regulator

The Attorney General of Vermont or to the Department of Financial Regulation, if regulated by the Department.

Threshold

If the breach requires notification of 1 or more Vermont residents.

Timing

Within 14 business days of discovery of the breach or when the covered entity provides notice to individuals, whichever is sooner.

Exemptions/Exceptions

HIPAA Exemption

A covered entity that is subject to the privacy, security, and breach notification rules under HIPAA is deemed to be in compliance with Vermont's data breach notification statute if:

- The covered entity experiences a breach that is limited to:
  - Health records or records of a wellness program or similar program of health promotion or disease prevention.
  - A healthcare professional's medical diagnosis or treatment of the consumer; or
  - A health insurance policy number.
- The covered entity provides notice to affected individuals pursuant to the requirements of the breach notification rule in HIPAA.

GLBA Exemption

A financial institution that is subject to the following guidance, and any revisions, additions, or substitutions relating to an interagency guidance, shall be exempt from Vermont's data breach notification statute:

- The Federal Interagency Guidance Response Programs for Unauthorized Access to Individual Information and Customer Notice, issued on March 7, 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;
- Final Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice, issued on April 14, 2005, by the National Credit Union Administration.

A financial institution regulated by the Department of Financial Regulation that is subject to the above shall notify the Department as soon as possible after it becomes aware of an incident involving unauthorized access to or use of personal information.

Risk of Harm

Notice is not required if the covered entity establishes that misuse of personal information is not reasonably possible. If the covered entity establishes that misuse of the personal information is not reasonably possible, the covered entity shall provide notice of its determination and a detailed explanation for said determination to the Vermont Attorney General or to the Department of Financial Regulation.

Good Faith/Employee Acquisition

Good faith but unauthorized acquisition of personally identifiable information or login credentials by an employee or agent of the covered entity for a legitimate purpose of the covered entity is not considered a breach, provided that the personally identifiable information or login credentials are not used for a purpose unrelated to the covered entity's business or subject to further unauthorized disclosure.

Encryption/Redaction

There is no breach when personal information is encrypted, redacted, or protected by another method that renders it unreadable or unusable.

Penalties/Private Right of Action

Private Right of Action

None.

Penalties

The Attorney General and State's Attorney or Department of Financial Regulation shall have sole and full authority to investigate potential violations of Vermont's data breach notification statute and to enforce, prosecute, obtain, and impose remedies for violations.

BakerHostetler

Virginia

Statute

Va. Code § 18.2-186.6

Covered Entities

An individual, corporation, business trust, estate, partnership, limited partnership, limited liability partnership, limited liability company, association, organization, joint venture, government, governmental subdivision, agency, instrumentality, or any other legal entity, whether for profit or not for profit, that owns, licenses, or maintains computerized data that includes personal information.

Quick Notes

- **Definition of Breach.** Unauthorized access and acquisition.
- **Notification Deadline.** Without unreasonable delay.
- **Regulatory Notice Required?** Yes, if the breach requires notification of 1 or more Virginia residents.
- **Risk of Harm Analysis?** Yes.
- **Applies to Paper Records?** No.

Definition of Personal Information

An individual's first name or first initial and last name in combination with and linked to any one or more of the following:

- Social Security number;
- Driver's license number or state identification card number issued in lieu of a driver's license number;
- Financial account number or credit card or debit card number in combination with any required security code, access code, or password that would permit access to a resident's financial accounts;
- Passport number; or
- Military identification number.

Definition of Breach

Unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes, or the individual or entity reasonably believes has caused or will cause, identity theft or other fraud to any Virginia resident.

Individual Notice

Timing

Without unreasonable delay.

Content

Notice shall include a description of the following:

- The incident in general terms;
- The type of personal information that was subject to the unauthorized access and acquisition;
- The general acts of the individual or entity to protect the personal information from further unauthorized access;
- A telephone number that the person may call for further information and assistance, if one exists; and
- Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports.

Method

- Written notice to the last known postal address in the covered entity's records;
- Telephone notice; or
- Electronic notice.

Substitute Notice

Substitute notice is permitted if the covered entity demonstrates one of the following:

- The cost of providing notice would exceed $50,000;
- The affected class of Virginia residents to be notified exceeds 100,000; or
- The covered entity does not have sufficient contact information.

Substitute notice shall consist of all of the following:

- E-mail notice when the covered entity has an e-mail address for the Virginia resident;
- Conspicuous posting of the notice on the covered entity's website, if the covered entity maintains one; and
- Notification to major statewide media.

Credit Monitoring

Not required.

Consumer Reporting Agency Notice

Threshold

If the breach requires notification of 1,000 or more Virginia residents, the covered entity must also notify all consumer reporting agencies of the timing, distribution, and content of the notice.

Timing

Without unreasonable delay.

Regulatory Notice

Regulator

The Attorney General of Virgina.

Threshold

If the breach requires notification of 1 or more Virginia residents.

Timing

Without unreasonable delay.

Exemptions/Exceptions

HIPAA Exemption

A covered entity that complies with the notification requirements or procedures pursuant to the rules, regulations, procedures, or guidelines established by the entity's primary or functional state or federal regulator shall be in compliance with Virginia's data breach notification statute.

GLBA Exemption

A covered entity that is subject to the GLBA and maintains procedures for notification of a breach of the security of the system in accordance with the GLBA shall be deemed to be in compliance with Virginia's data breach notification statute.

Risk of Harm

Notice is not required if unauthorized access and acquisition does not cause, or the covered entity reasonably believes has not caused or will not cause, identity theft or another fraud to any Virginia resident.

Good Faith/Employee Acquisition

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

Encryption/Redaction

There is no breach when the information involved in the incident was secured by encryption or redaction such that the data was unreadable or unusable.

Penalties/Private Right of Action

Private Right of Action

Virginia law allows individuals to pursue civil remedies to recover direct economic damages.

Penalties

The Attorney General may bring an action to address violations of Virginia's data breach notification statute. The Office of the Attorney General may impose a civil penalty not to exceed $150,000 per breach of the security of the system or a series of breaches of a similar nature that are discovered in a single investigation.

Other

Related Laws

Pursuant to Va. Code § 32.1-127.1:05, "Medical Information" means the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a Virginia resident, when the data elements are neither encrypted nor redacted:

- Information regarding an individual's medical or mental health history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional; or
- Individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

Where a breach occurs involving Medical Information that is not subject to federal law, the statute requires the data owner to provide notice to the Office of the Virginia Attorney General, the Virginia Commissioner of Health, the subject of the Medical Information, and any affected Virginia resident without unreasonable delay.

Pursuant to Va. Code § 22.1-287.02, in cases in which electronic records containing personally identifiable information (as defined under FERPA) are reasonably believed by the Department of Education or a local school division to have been disclosed in violation of FERPA, the Department or local school division shall notify, as soon as practicable, the parent of any student affected by such disclosure. Such notification shall include the:

- Date, estimated date, or date range of the disclosure;
- Type of information that was or is reasonably believed to have been disclosed; and
- Remedial measures taken or planned in response to the disclosure.

Additional Provisions

An employer or payroll service provider must notify the Virginia Attorney General without unreasonable delay after discovery of a breach of computerized data containing a Virginia resident's taxpayer identification number (TIN), combined with income tax withheld. The notification must include the name and TIN of the affected Virginia residents. For an employer, this applies to information concerning employees only. Notification is not required when the employer or payroll service provider reasonably believes that the breach has not and will not cause identity theft or other fraud.

important decision that should not be based solely upon advertisements. Before you decide, ask us to send you written information about our qualifications and experience.

BakerHostetler

Washington

Statute

Wash. Rev. Code § 19.255.010 et seq.; Wash. Rev. Code § 42.56.590

Covered Entities

Any person or business that maintains or possesses data that may include personal information, or any person or business that conducts business in Washington and owns or licenses data that includes personal information.

Quick Notes

- **Definition of Breach.** Unauthorized acquisition.
- **Notification Deadline.** 30 days after discovery of the breach.
- **Regulatory Notice Required?** Yes, if the breach requires notification of 500 or more Washington residents.
- **Risk of Harm Analysis?** Yes.
- **Applies to Paper Records?** No.

Definition of Personal Information

An individual's first name or first initial and last name in combination with any one or more of the following:

- Social Security number;
- Driver's license number or Washington identification card number;
- Account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account, or any other numbers or information that can be used to access a person's financial account;
- Full date of birth;
- Private key that is unique to an individual and that is used to authenticate or sign an electronic record;
- Student, military, or passport identification number;
- Health insurance policy number or health insurance identification number;
- Any information about a consumer's medical history or mental or physical condition or about a healthcare professional's medical diagnosis or treatment of the consumer;
- Biometric data; or
- Username or e-mail address in combination with a password or security question and answer that would permit access to an online account; and

Any of the data elements or any combination of the data elements described above without the

consumer's first name or first initial and last name, if:

- Encryption, redaction, or other methods have not rendered the data element or combination of data elements unusable; and
- The data element or combination of data elements would enable a person to commit identity theft against a consumer.

Definition of Breach

Unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal information maintained by the covered entity.

Individual Notice

Timing

In the most expedient time possible and without unreasonable delay, but no more than 30 calendar days after the breach was discovered.

Content

The notice shall, at minimum, include:

- The name and contact information of the covered entity;
- A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;
- A time frame of exposure, if known, including the date of the breach and the date of the discovery of the breach; and
- The toll-free telephone numbers and addresses of the major credit reporting agencies, if the breach exposed personal information.

Method

- Written notice; or
- Electronic notice, if the notice provided is consistent with the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001 et seq.).

Substitute Notice

Substitute notice is permitted if the covered entity demonstrates one of the following:

- The cost of providing notice would exceed $250,000;
- The affected class of Washington residents to be notified exceeds 500,000; or
- The covered entity does not have sufficient contact information.

Substitute notice shall consist of all of the following:

- E-mail notice when the person or business has an e-mail address for the subject persons;
- Conspicuous posting of the notice on the covered entity's website, if the covered entity maintains one; and
- Notification to major statewide media.

Credit Reporting

None required.

Consumer Reporting Agency Notice

Threshold

CRA notice is not required.

Timing

N/A

Regulatory Notice

Regulator

The Attorney General of Washington.

Threshold

If the breach requires notification of 500 or more Washington residents.

Timing

Within no more than 30 days after the breach was discovered.

Exemptions/Exceptions

HIPAA Exemption

A covered entity under HIPAA is deemed to have complied with Washington's breach notification statute with respect to protected health information if it has complied with Section 13402 of HITECH as it existed on July 24, 2015.

Covered entities shall notify the Attorney General pursuant to RCW 19.255.010(7) in compliance with the timeliness of notification requirements of Section 13402 of HITECH.

GLBA Exemption

A financial institution under the authority of the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the National Credit Union Administration, or the Federal Reserve System is deemed to have complied with the requirements of Washington's breach notification law with respect to "sensitive customer information" if the financial institution provides notice to affected Washington residents pursuant to the Interagency Guidelines and Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice under 12 C.F.R. Part 364 as it existed on July 24, 2015.

The covered entity shall notify the Washington Attorney General pursuant to RCW 19.255.010 in addition to providing notice to its primary federal regulator.

Risk of Harm

Notification is not required if the breach is not reasonably likely to subject consumers to a risk of harm.

Good Faith/Employee Acquisition

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

Encryption/Redaction

There is no breach when the information involved in the incident was secured by encryption, redaction, or some other method or technology that rendered the data unreadable, unusable, or undecipherable.

Penalties/Private Right of Action

Private Right of Action

Any consumer injured by a violation of Washington's breach notification statute may institute a civil action to recover damages.

Penalties

The Washington Attorney General may bring an action against the covered entity for a violation of Washington's breach notification statute.

BakerHostetler

West Virginia

Statute

W. Va. Code § 46A-2A-101, et seq.

Covered Entities

Any natural person, corporation, business trust, estate, 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, that owns, licenses, or maintains computerized data that includes personal information.

Quick Notes

- **Definition of Breach.** Unauthorized access and acquisition.
- **Notification Deadline.** As soon as practicable.
- **Regulatory Notice Required?** No.
- **Risk of Harm Analysis?** Yes.
- **Applies to Paper Records?** No.

Definition of Personal Information

First name or first initial and last name linked to any one or more of the following:

- Social Security number;
- Driver's license number or state identification card number issued in lieu of a driver's license; and
- Financial account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to a resident's financial accounts.

Definition of Breach

Unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes the individual or entity to reasonably believe that the breach of security has caused or will cause identity theft or other fraud to any resident of West Virginia.

Individual Notice

Timing

As soon as practicable following discovery.

Content

- To the extent possible, a description of the categories of information that were reasonably believed to have been accessed or acquired by an unauthorized person, including Social Security numbers, driver's licenses or state identification numbers, and financial data;
- A telephone number or website address that the individual may use to contact the entity or the agent of the entity and from whom the individual may learn:
  - The types of information the entity maintained about that individual or about individuals in general; and
  - Whether or not the entity maintained information about that individual.
- Toll-free contact telephone numbers and addresses for the major credit reporting agencies and information on how to place a fraud alert or security freeze.

Method

- Written notice to the postal address in the records of the individual or entity;
- Telephonic notice; or
- Electronic notice for those consumers for whom the person has valid e-mail addresses and who have agreed to receive communications electronically, if the notice provided is consistent with the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001 et seq.).

Substitute Notice

Substitute notice is permitted if the covered entity demonstrates one of the following:

- The cost of providing notice would exceed $50,000;
- The affected class of subject persons to be notified exceeds 100,000 West Virginia residents; or
- The covered entity does not have sufficient contact information.

Substitute notice shall consist of any two of the following:

- E-mail notice when the covered entity has e-mail addresses for the subject persons;
- Conspicuous posting of the notice on the covered entity's website, if the covered entity maintains one; and
- Notification to major statewide media.

Credit Monitoring

Not required.

Consumer Reporting Agency Notice

Threshold

If the breach requires notification to 1,000 or more residents, the covered entity must notify the consumer reporting agencies of the timing, distribution, and content of the notice given to the West Virginia residents.

Timing

As soon as practicable.

Regulatory Notice

Regulator

None.

Threshold

N/A

Timing

N/A

Exemptions/Exceptions

HIPAA Exemption

A covered entity that complies with the notification requirements or procedures pursuant to the rules, regulations, procedures, or guidelines established by the entity's primary or functional regulator shall be in compliance with West Virginia's breach notification statute.

GLBA Exemption

A financial institution that responds in accordance with the notification guidelines prescribed by the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice is deemed to be in compliance with West Virginia's breach notification statute.

Risk of Harm

Notification is not required if the covered entity reasonably believes that the breach of security has not caused or will not cause identity theft or other fraud to any resident of West Virginia.

Good Faith/Employee Acquisition

Good faith acquisition of personal information by an employee or agent of the covered entity is not a breach if the personal information is not used for a purpose other than the lawful purpose of the covered entity and is not subject to further unauthorized disclosure.

Encryption/Redaction

Notification is not required if the computerized data is encrypted or redacted such that it is unreadable or unusable.

Penalties/Private Right of Action

Private Right of Action

None.

Penalties

Failure to comply with the notice provisions of West Virginia's breach notification statute constitutes an unfair or deceptive act. The Attorney General has authority to bring an action under the Unfair Trade Practices and Consumer Protection Law for statutory violations.

No civil penalty may be assessed in an action unless the court finds that the covered entity has engaged in a course of repeated and willful violations of West Virginia's breach notification statute. No civil penalty shall exceed $150,000 per breach of security of the system or series of breaches of a similar nature that are discovered in a single investigation.

BakerHostetler

Wisconsin

Statute

Wis. Stat. § 134.98

Covered Entities

An individual or entity that owns, maintains, or stores personal information pertaining to Wisconsin residents.

Quick Notes

- **Definition of Breach.** Unauthorized acquisition.
- **Notification Deadline.** Within 45 days of the discovery of the breach.
- **Regulatory Notice Required?** No.
- **Risk of Harm Analysis?** Yes.
- **Applies to Paper Records?** Yes.

Definition of Personal Information

An individual's first name or first initial and last name in combination with and linked to any of the following:

- The individual's Social Security number;
- The individual's driver's license number or state identification number;
- The individual's financial account number, including a credit or debit card number or any security code, access code, or password that would permit access to the individual's financial account;
- The individual's DNA profile;
- The individual's unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation.

Definition of Breach

When a covered entity knows that personal information in the entity's possession has been acquired by a person whom the entity has not authorized to acquire the personal information.

Individual Notice

Timing

Within a reasonable time, but not to exceed 45 days.

Content

The notice shall indicate that the entity knows of the unauthorized acquisition of personal information pertaining to the Wisconsin resident.

Method

By mail or by a method the entity has previously employed to communicate with the subject of the personal information.

Substitute Notice

If a covered entity cannot, with reasonable diligence, determine the mailing address of the subject of the personal information, and if the entity has not previously communicated with the subject of the personal information, the covered entity shall provide notice by a method reasonably calculated to provide actual notice to the subject of the personal information.

Consumer Reporting Agency Notice

Threshold

If the breach requires notification of 1,000 or more Wisconsin residents.

Timing

Without unreasonable delay.

Regulatory Notice

Regulator

None.

Threshold

N/A

Timing

N/A

Exemptions/Exceptions

HIPAA Exemption

Wisconsin's data breach notification statute does not apply to an entity that is described in 45 CFR 164.104(a), if the entity complies with the requirements of the HIPAA Privacy Rule.

GLBA Exemption

Wisconsin's data breach notification statute does not apply to an entity that is subject to and in compliance with the privacy and security requirements of 15 USC 6801 to 6827, or a person that has a contractual obligation to such an entity, if the entity or person has a policy concerning breaches of information security in effect.

Risk of Harm

A covered 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.

Good Faith/Employee Acquisition

A covered entity is not required to provide notice of the acquisition of personal information if the personal information was acquired in good faith by an employee or agent of the covered entity, if the personal information is used for a lawful purpose of the entity.

Encryption/Redaction

Wisconsin's data breach notification statute does not apply to information that is encrypted, redacted, or altered in a manner that renders the data unreadable.

Penalties/Private Right of Action

Private Right of Action

Wisconsin's data breach notification statute does not explicitly provide for a private right of action, but it provides that, while a violation itself is not negligence or a breach of any duty, it may be evidence of negligence or a breach of a legal duty.

Penalties

A violation of Wisconsin's data breach notification statute may result in civil penalties.

BakerHostetler

Wyoming

Quick Notes

- **Definition of Breach.** Unauthorized acquisition.
- **Notification Deadline.** Without unreasonable delay.
- **Regulatory Notice Required?** No.
- **Risk of Harm Analysis?** Yes.
- **Applies to Paper Records?** No.

Statute

Wyo. Stat. § 40-12-501 et seq.

Covered Entities

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

Definition of Personal Information

An individual's first name or first initial and last name in combination with one or more of the following:

- Social Security number;
- Driver's license number;
- Account number or credit or debit card number in combination with any security code, access code, or password that would permit access to an individual's financial account;
- Tribal ID card;
- Federal or state government-issued identification card;
- Shared secrets or security tokens that are known to be used for data-based authentication;
- A username or e-mail address in combination with a password or security question and answer that would permit access to an online account;
- A birth or marriage certificate;
- Medical information, meaning a person's medical history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional;
- Health insurance information, meaning a person's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the person, or information related to a person's application and claims history;
- Unique biometric data, meaning data generated from measurements or analysis

of human body characteristics for authentication purposes; or

- An individual Taxpayer Identification Number.

Definition of Breach

Unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personally identifying information maintained by a covered entity and causes or is reasonably believed to cause loss or injury to a Wyoming resident.

Individual Notice

Timing

Notice shall be made in the most expedient time possible and without unreasonable delay.

Content

Individual notice shall be clear and conspicuous and shall include, at a minimum, the following:

- A toll-free number that the individual may use to contact the person collecting the data or his agent and from whom the individual may learn the toll-free contact telephone numbers and addresses for the major credit reporting agencies;
- The types of personally identifying information that were or are reasonably believed to have been the subject of the breach;
- A general description of the breach incident;
- The approximate date of the breach of security, if that information is reasonably possible to determine at the time notice is provided;
- In general terms, the actions taken by the individual or commercial entity to protect the system containing the personally identifying information from further breaches;
- Advice that directs the person to remain vigilant by reviewing account statements and monitoring credit reports;
- Whether notification was delayed as a result of a law enforcement investigation, if that information is reasonably possible to determine at the time the notice is provided.

Method

- Written notice; or
- Electronic mail notice.

Substitute Notice

Substitute notice is permitted if the covered entity demonstrates one of the following:

- The cost of providing notice would exceed $10,000 for Wyoming-based persons or businesses and $250,000 for all other businesses operating but not based in Wyoming;
- The affected class of subject persons to be notified exceeds 10,000 for Wyoming-based persons or businesses and 500,000 for all other businesses operating but not based in Wyoming; or
- The covered entity does not have sufficient contact information.

Substitute notice shall consist of all of the following:

- Conspicuous posting of the notice on the covered entity's website, if the covered entity maintains one; and
- Notification to major statewide media. The notice to media shall include a toll-free phone number where an individual can learn whether or not that individual's personal data is included in the security breach.

Credit Monitoring

Not required.

Consumer Reporting Agency Notice

Threshold

CRA notice not required.

Timing

N/A

Regulatory Notice

Regulator

None.

Threshold

N/A

Timing

N/A

Exemptions/Exceptions

HIPAA Exemption

A covered entity that is subject to and complies with HIPAA is deemed to be in compliance with this section if the covered entity or business associate notifies affected Wyoming customers or entities in compliance with the requirements of HIPAA.

GLBA Exemption

Any financial institution or federal credit union pursuant to the GLBA that maintains notification procedures subject to the requirements of the GLBA is deemed to be in compliance with Wyoming's breach notification statute if the covered entity notifies affected Wyoming residents in compliance with the requirements of the GLBA.

Risk of Harm

Notification is not required if an investigation determines that the misuse of information about a Wyoming resident has not occurred or is not reasonably likely to occur.

Good Faith/Employee Acquisition

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

Encryption/Redaction

There is no breach when the information involved in the incident was redacted such that it is not readable or usable.

Penalties/Private Right of Action

Private Right of Action

None.

Penalties

The Wyoming Attorney General may bring an action in law or equity to address any violation of Wyoming's breach notification statute, and for other relief that may be appropriate to ensure proper compliance with Wyoming's breach notification statute, to recover damages, or both. The provisions of Wyoming's breach notification statute are not exclusive and do not relieve a covered entity from compliance with all other applicable provisions of law.

important decision that should not be based solely upon advertisements. Before you decide, ask us to send you written information about our qualifications and experience.