BakerHostetler

Alabama

Act No. 2018-396 (2018)

Quick Notes

- "Personal Information" is broader than the general definition.
- Notification is not triggered by only access.
- A risk of harm analysis is permitted in determining when notification is triggered.
- If more than 1,000 individuals are affected, notice to the Attorney General is required no later than 45 days after the covered entity receives notice of a breach (from a third-party agent) or becomes aware that a breach has occurred.
- Notification is required within 45 days of notice from a third-party agent or upon determination that a breach has occurred.
- A private cause of action is not permitted.
- There is an encryption safe harbor.
- The law does not apply to paper records.

Personal Information Definition (i.e.,"Sensitive PII")

An individual's first name or first initial and last name plus one or more of the following data elements:

1. Social Security number.

2. Driver's license number or state-issued ID card number.

3. Account number, credit card number or debit card number.

4. Tax identification numbers, passport numbers, military identification numbers and other unique identification numbers issued on a government document used to verify the identity of a specific individual.

5. Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional.

6. Health insurance policy number or subscriber identification number, and any unique identifier used by a health insurer to identify the individual.

7. A username or email address in combination with a password or a 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.

Persons Covered

A person … government entity … corporation, nonprofit … estate … or other business entity that acquires or uses sensitive PII.

Encryption/Notification Trigger

The statute only applies to unencrypted information. If the encryption key that makes personal information readable has been breached, the statute applies to information that is encrypted, truncated, secured or modified.

Standard for Triggering: The statute is triggered when an investigation reveals personal information has been acquired or is reasonably believed to have been acquired by an unauthorized person, and is "reasonably likely to cause substantial harm to the individuals to whom the information relates."

If a covered entity determines that notice is not required, the covered entity shall document the determination in writing and maintain records of the determination for no less than five years.

Specific Content Requirements

The notice shall include:

1. The date or estimated date range of the breach.
2. A description of the sensitive PII that was acquired by an unauthorized person.
3. A description of the actions taken by a covered entity to restore the security of the affected personal information.
4. A description of steps an affected individual can take to protect himself or herself from identity theft.
5. Information that the individual can use to contact the covered entity to inquire about the breach.

Timing

If the breach is “reasonably likely to cause substantial harm to individuals,” then notice must be provided expediently and without unreasonable delay, but within 45 days, subject to the needs of law enforcement.

If a third-party agent has experienced a breach, the agent shall notify the covered entity as soon as possible, but within 10 days of becoming aware of the breach’s occurrence, and provide information relevant to the breach.

Penalty/Private Right of Action

The statute does not create a private right of action.

Violations of the notification provisions are “unlawful trade practices” under the Alabama Deceptive Trade Act, Chapter 19, Title 8.

Covered entities may be liable for a civil penalty of not more than $5,000 per day for each consecutive day the covered entity fails to notify affected individuals. The Attorney General may bring an action on behalf of any named individuals, in which recovery is limited to actual damages suffered by the individuals plus reasonable attorneys’ fees and costs.

“Knowingly” violating the statute may subject a covered entity to additional penalties under § 8-19-11.

Government entities are exempt from the civil penalties, but may be subject to injunctive remedies.

Other Provisions

If a covered entity is required to notify more than 1,000 individuals, the covered entity shall provide written notice to the Attorney General within 45 days. Written notice to the Attorney General shall include:

1. A synopsis of the events surrounding the breach.
2. The approximate number of individuals in the state who were affected.
3. Any services related to the breach being offered or scheduled to be offered.
4. The name, address, telephone number and email address of the employee or agent of the covered entity from whom additional information may be obtained.

If a covered entity is required to notify more than 1,000 individuals, the covered entity must notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.

BakerHostetler

Alaska

Alaska Stat. Tit. 45.48.010 et seq.

Quick Notes

- "Personal Information" is broader than the general definition.
- Notification is not triggered by only access.
- A risk of harm analysis is permitted in determining when notification is triggered.
- Notice of a risk of harm determination is required to the Attorney General if the covered entity determines "no reasonable likelihood of harm" to the consumers has resulted or will result from the breach.
- Notice is not required within an explicit number of days, but it must be made in the most expeditious time possible and without unreasonable delay.
- A private cause of action is permitted under the Unfair or Deceptive Act or Practices, AS 45.50.471 – 45.50.561.
- There is an encryption safe harbor, unless the encryption key has been disclosed.
- The law applies to electronic and paper records.

Personal Information Definition

An individual's first name or first initial and last name plus one or more of the following data elements:

1. Social Security number.

2. Driver's license number or state-issued ID card number.

3. Account number, credit card number or debit card number.

4. Passwords, personal identification numbers or other access codes for financial accounts.

Persons Covered

Any person doing business, government agency or person with more than 10 employees who owns, licenses or maintains unencrypted personal information about Alaska residents.

Encryption/Notification Trigger

The statute only applies to unencrypted information or encrypted information when the encryption key has also been disclosed.

Standard for Triggering: The statute is triggered when a covered person discovers or is notified of a breach of security.

Notice is not required if there is not "a reasonable likelihood that harm to the consumers … has resulted or will result from the breach." The determination, following a reasonable investigation, must be documented in writing and maintained for five years.

Specific Content Requirements

None.

Timing

Notification must be provided expeditiously and without "unreasonable delay."

Law enforcement may delay notification. If such a delay occurs, notification must be made after law enforcement determines that it will not interfere with an investigation.

An "information recipient" involved in the breach must notify the information distributor who owns or licensed the personal information about the breach.

Penalty/Private Right of Action

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 this statute is an “unfair or deceptive act or practice” under AS 45.50.471-45.50.561 if the violator was an information collector who is not a government agency.

The information collector is not subject to civil penalties imposed under 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 AS 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 information collector under AS 45.50.531 are limited to actual economic damages that do not exceed $500.

Other Provisions

If over 1,000 Alaska residents must be notified, the information collector must also notify all nationwide consumer reporting agencies (unless the information collector is subject to the Gramm-Leach-Bliley Financial Modernization Act).

BakerHostetler

Arizona

Ariz. Rev. Stat. § 44-7501 (2006); as amended (2007, 2016, 2018)

Quick Notes

- "Personal Information" is broader than the general definition.
- Notification is not triggered by only access.
- A risk of harm analysis is permitted in determining when notification is triggered.
- If more than 1,000 individuals must be notified of the breach, notice must be made to the Attorney General and the three largest nationwide consumer reporting agencies.
- Notice is required within 45 days after the determination that there has been a security system breach.
- A private cause of action is not permitted.
- There is an encryption safe harbor.
- The law does not apply to paper records.

Personal Information Definition

An individual's first name or first initial and last name plus one or more of the following data elements:

1. Social Security number.

2. Driver's license number or state-issued ID card number.

3. Account number, credit card number or debit card number.

4. A private key unique to an individual that is used to sign or authenticate an electronic record.

5. A health insurance identification number.

6. Information about an individual's medical or mental health treatment or diagnosis by a healthcare professional.

7. Passport number.

8. A taxpayer identification number or an identity protection personal identification number issued by the IRS.

9. Unique biometric data generated from a measurement or analysis of human body characteristics to authenticate an individual when the individual accesses an online account.

10. A username or email address, in combination with a password or a security question and answer that allows access to an online account.

Persons Covered

Any natural person, corporation … estate, trust, partnership … governmental subdivision, or agency or any other legal or commercial entity that conducts business in Arizona and owns, maintains, or licenses unencrypted and unredacted computerized personal information that becomes aware of a security incident.

Encryption/Notification Trigger

Notification requirement only applies where personal information was unencrypted and/or unredacted.

Standard for Triggering: The statute is triggered when an investigation results in a determination that there has been a security system breach.

Notice is not required if the breach has not resulted in or is not reasonably likely to result in substantial economic loss to affected individuals.

Specific Content Requirements

The notification must include (1) the approximate date of the breach, (2) a brief description of the personal information included in the breach, (3) the toll-free numbers and addresses for the three largest

nationwide consumer reporting agencies and (4) the toll-free number, address and website address, for the federal trade commission, of any federal agency that assists consumers with identity theft matters.

Notification shall be provided by (1) written notice, (2) an email notice if the person has email addresses for the individuals who are subject to the notice, (3) telephonic notice if telephonic contact is made directly with the affected individuals and is not through a prerecorded message or (4) substitute notice (if costs of delivering notice exceed $50,000, the affected class of individuals exceeds 100,000 individuals or the person does not have sufficient contact information).

Timing

In the most expedient manner possible without unreasonable delay. Notification to the affected individuals must be made within 45 days.

An entity that maintains personal information that it does not own shall notify the owner of the information pursuant to this section. The person who maintains the data under an agreement with the owner or licensee is not required to provide notifications to the individual unless the agreement stipulates otherwise.

Notification may be delayed if it would impede a criminal investigation. The entity shall make the required notifications within 45 days after being informed by the law enforcement agency that the notifications no longer compromise the investigation.

Penalty/Private Right of Action

The section is exclusively enforced by the Attorney General, who may bring an action to obtain actual damages for a willful and knowing violation, and a civil penalty not to exceed $10,000 per breach or series of similar breaches discovered in a single investigation. The Attorney General may also recover restitution for affected individuals.

The Attorney General may impose a civil penalty for a violation, not to exceed the lesser of $10,000 per affected individual or the total amount of economic loss sustained by affected individuals. However, the maximum civil penalty from a breach or series of related breaches may not exceed $500,000. The Attorney General may also recover restitution for the affected individuals.

Other Provisions

If the breach requires notification of more than 1,000 individuals, notification must be made to the three largest nationwide consumer reporting agencies and the Attorney General.

BakerHostetler

Arkansas

Ark. Code Ann. §§ 4-110-101-108 (2005)

Quick Notes

- "Personal Information" is broader than the general definition.
- Notification is not triggered by only access.
- A risk of harm analysis is permitted in determining when notification is triggered.
- Notice to the Attorney General or State Agency is not required.
- Notice is not required within an explicit number of days, but it must be given in the most expedient time and manner possible and without unreasonable delay.
- A private cause of action is not permitted.
- There is an encryption safe harbor.
- The law does not apply to paper records, except for medical information.

Personal Information Definition

An individual's first name or first initial and last name plus one or more of the following data elements:

1. Social Security number.

2. Driver's license number or state-issued ID card number.

3. Account number, credit card number or debit card number.

4. Medical information, defined as any individually identifiable information, in electronic or physical form, regarding the individual's medical history or medical treatment or diagnosis by a health care professional

Persons Covered

Any person or business who acquires, owns, licenses or maintains computerized data that includes personal information about Arkansas residents.

Encryption/Notification Trigger

The statute only applies to unencrypted data elements.

Standard for Triggering: The statute is triggered upon discovery of an unauthorized acquisition of personal information maintained by a covered entity if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Notification under this section is not required if, after a reasonable investigation, the person or business determines that there is no reasonable likelihood of harm to customers.

Specific Content Requirements

None.

Timing

Covered entities must give notice in the most expedient time and manner possible and without unreasonable delay, subject to the needs of law enforcement.

Covered entities that maintain personal information that the entity does not own shall notify the owner or licensee of the information immediately following discovery of a breach if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Penalty/Private Right of Action

Any violation of this statute is punishable by action of the Attorney General.

A covered entity that “knowingly” and “willfully” commits an unlawful practice under [the Personal Information Protection Act] shall be guilty of a Class A misdemeanor.

The Attorney General has the authority, acting through the consumer counsel, to file an action for civil enforcement of the provisions of this chapter, including, but not limited to, the seeking of restitution and the seeking of an injunction prohibiting any person from engaging in any deceptive or unlawful practice prohibited by this statute.

Other Provisions

None.

BakerHostetler

California

Calif. Civ. Code §§ 1798.29, 1798.80, 1798.82 (as amended, 2016), 1798.84; Calif. Health and Safety Code § 1280.15 (2015)

Quick Notes

- "Personal Information" is broader than the general definition.
- Notification is not triggered by only access.
- A risk of harm analysis is not permitted in determining when notification is triggered.
- Under the general breach notification statute, notice to the Attorney General or State Agency is required in a specific format if more than 500 California residents must be notified. Under the medical information specific breach notification statute, the California Department of Health Services must be notified no later than 15 business days after the detection of a breach.
- Under the general breach notification statute, notice is not required within an explicit number of days. Under the medical information specific breach notification statute, affected individuals and the California Department of Health Services must be notified no later than 15 business days after a breach of security.
- Under the general breach notification statute, a private cause of action is permitted. Under the medical information specific breach notification statute, a private cause of action is not permitted.
- There is an encryption safe harbor, unless the encryption key has been exposed by the breach.
- The law does not apply to paper records.

Personal Information Definition

Under the general breach notification statute, PI is an individual's first name or first initial and last name plus one or more of the following data elements:

1. Social Security number.

2. Driver's license number or state-issued ID card number.

3. Account number, credit card number or debit card number.

4. A username or email address in combination with a password or a security question and answer that would permit access to an online account.

5. Information or data collected through the use or operation of an automated license plate recognition system.

6. Medical information and health insurance information.

The Medical Information Specific Breach Notification Statute protects "Medical Information" (see full text statute).

Persons Covered

Any state agency, person or business who conducts business in California and owns, licenses or maintains computerized data that includes personal information is covered under the General Breach Notification Statute.

Clinics, health facilities, home health agencies and hospices licensed pursuant to sections 1204, 1250, 1725 or 1745 of the California Health and Safety Code are covered under the Medical Information Specific Breach Notification Statute.

Encryption/Notification Trigger

The General Breach Notification Statute applies where the information is either (a) not encrypted or (b) encrypted, if an encryption key or security credential that allows an unauthorized party to render the data readable or usable is also compromised.

Standard for Triggering: The statute is triggered upon discovery or notification of the unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal information maintained by the entity.

The Medical Information Specific Breach Notification Statute is triggered by any unlawful or unauthorized access to, or use or disclosure of, a patient's medical information.

Specific Content Requirements

Under the General Breach Notification Statute, notification to California residents must be in written form, using plain language in no smaller

than 10-point type. The notification shall be titled “Notice of Data Breach” and use all of the following clearly and conspicuously displayed headings:

(1) “What Happened”

(2) “What Information Was Involved”

(3) “What We Are Doing”

(4) “What You Can Do”

(5) “For More Information”

The breach notification must include four elements: (1) the date of the notice; (2) the name and contact information of the person reporting a breach; (3) a list of the types of personal information likely impacted; and (4) if the breach exposed a Social Security number or a driver’s license or CA identification card number, the toll-free telephone numbers and addresses of the major credit reporting agencies.

If the breach may have exposed Social Security numbers or driver’s license or CA identification card numbers, the entity must provide appropriate identity theft protection and mitigation services at no cost to the affected persons for not less than 12 months.

If the breach only involved a username or email address in combination with a password or security question permitting access to an online account, notice to CA residents may be in electronic or other form that directs the affected individual to promptly change his or her password and security question answer or take other precautionary security steps.

If the breach involved login credentials of an email account furnished by an entity, the entity must provide notice to that email address as well as by another “clear and conspicuous” method, delivered to the resident online when the resident is connected to the online account from an IP address or online location from which the entity knows the resident customarily accesses the account.

Timing

Under the General Breach Notification Statute, disclosure shall be made “expediently” and without “unreasonable delay,” consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the integrity of the data system.

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

Under the Medical Information Specific Breach Notification Statute, affected patients and the California Department of Health Services must be notified no later than 15 business days after the unauthorized access, use or disclosure has been detected by the licensee. This notice can be delayed for law enforcement purposes so long as the delay is documented in accordance with the requirements of section 1280.15(c) of the California Health and Safety Code.

Penalty/Private Right of Action

Under the General Breach Notification Statute, any customer injured by a violation of § 1798.82 may institute a civil action to recover damages. Also, any business that violates or proposes to violate § 1798.82 may be enjoined.

There is a “Safe Harbor Exception” for a record custodian who properly disposes of records.

Under the Medical Information Specific Breach Notification Statute, the California Department of Health Services may impose the following penalties against licensees who violate section 1280.15:

(1) $25,000 per patient whose information was affected, and up to $17,500 per subsequent occurrence.

(2) Entities that fail to report the incident to the State Department of Health Services or the affected patients within the 15-day time period absent lawful delay are subject to a penalty of $100 per day.

(3) The total penalties imposed may not exceed $250,000 per reported event.

Other Provisions

Under the General Breach Notification Statute, any person who notifies more than 500 California residents as a result of a single breach must complete and submit the Attorney General's Data Security Breach form, and attach a single sample copy of the notification letter sent to the affected California residents.

Under the Medical Information Specific Breach Notification Statute, the California Department of Health Services must be notified no later than 15 business days after the unauthorized access, use or disclosure has been detected by the licensee.

BakerHostetler

Colorado

Colo. Rev. Stat. Ann. § 6-1-716 (2006); as amended (2018)

Quick Notes

- "Personal Information" is broader than the general definition.
- Notification is not triggered by only access.
- A risk of harm analysis is permitted in determining when notification is triggered.
- If 500 Colorado residents or more were affected by the breach, notice to the Attorney General is required not later than 30 days after the date of determination that a security breach occurred.
- Notice is required not later than 30 days after the date of determination that a security breach occurred.
- A private cause of action is not permitted.
- There is an encryption safe harbor, unless the encryption key was exposed by the breach.
- The law does not apply to paper records.

Personal Information Definition

An individual's first name or first initial and last name plus one or more of the following data elements:

1. Social Security number.

2. Driver's license number or state-issued ID card number.

3. Any student, military or passport identification number.

4. Medical information.

5. Health insurance identification number.

6. Biometric data.

In addition, the following elements are considered personal information even when not combined with an individual's name:

1. A username or email address in combination with a password or security questions and answers that would permit access to an online account.

2. A 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 that account.

Persons Covered

An individual, corporation, … estate, … unincorporated association or commercial entity that (a) conducts business in Colorado and that owns or licenses computerized data that includes personal information about a Colorado resident, or (b) maintains computerized data that includes personal information that the person or entity does not own or license.

Encryption/Notification Trigger

The statute only applies to unencrypted information. If the encryption key or other means used to decipher the secured information was also acquired in the security breach, then the statute also applies to encrypted information.

Standard for Triggering: The statute is triggered when a covered entity becomes aware that a security breach may have occurred.

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

Specific Content Requirements

1. Notice to affected Colorado residents must include, but need not be limited to, the following information:

2. The date, estimated date or estimated date range of the security breach.

3. A description of the personal information that was acquired or reasonably believed to have been acquired as part of the security breach.

4. Information that the resident can use to contact the covered entity or governmental entity to inquire about the security breach.

5. The toll-free numbers, addresses and websites for consumer reporting agencies.

6. The toll-free number, address and website for the Federal Trade Commission.

7. A statement that the resident can obtain information from the Federal Trade Commission and the credit reporting agencies about fraud alerts and security freezes.

If the breach involved login credentials (i.e., usernames, passwords and security questions), then the entity must direct the affected individual to promptly change his or her password and security question(s), or to take other precautionary steps.

If the login credentials of an email account furnished by the covered entity are impacted, the covered entity shall not provide notice to that email address, but may provide notice through another method, including conspicuous notice to the resident online when the resident is connected to the online account or online location from which the covered entity knows the resident customarily accesses the account.

Timing

Notice shall be made expediently and without “unreasonable delay,” but not later than 30 days, subject to the needs of law enforcement.

A third-party service provider that maintains personal information on behalf of a covered entity shall give expeditious notice to and cooperate with the covered entity in the event of a security breach. A third-party service provider must share information with the covered entity relevant to the security breach.

Notice may be delayed if the notice will impede a criminal investigation and the law enforcement agency has notified the entity that conducts business in Colorado not to send notice. Notice must be made no later than 30 days after law enforcement has notified the entity that it is appropriate to send the required notice.

Penalty/Private Right of Action

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

Other Provisions

If the breach affected more than 500 residents, then a covered entity must provide notice to the Colorado Attorney General within 30 days.

If the covered entity is required to notify more than 1,000 Colorado residents, the entity must notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.

BakerHostetler

Connecticut

Conn. Gen. Stat. § 36A-701B (2005); as amended (2012, 2015, 2018)

Quick Notes

- "Personal Information" is not broader than the general definition.
- Notification is triggered by only access.
- A risk of harm analysis is permitted in determining when notification is triggered.
- If notice of a breach of security is required to be provided to affected individuals, the person must also provide notice of the breach to the Attorney General not later than the time when notice is provided to residents.
- All licensees and registrants of the Connecticut Insurance Department are required to notify the department of any breach "as soon as the incident is identified," but no later than five calendar days after the incident is identified.
- Notice is required within 90 days after the determination that there has been a security system breach.
- A private cause of action is not permitted.
- There is an encryption safe harbor.
- The law does not apply to paper records.

Personal Information Definition

An individual's first name or first initial and last name plus one or more of the following data elements:

1. Social Security number.

2. Driver's license number or state-issued ID card number.

3. Account number, credit card number or debit card number.

Persons Covered

Any person, business or agency who conducts business in Connecticut, and who, in the ordinary course of such entity's business, owns, licenses or maintains computerized data that includes personal information.

Encryption/Notification Trigger

A breach of security only applies to unencrypted information.

Standard for Triggering: The statute is triggered upon discovery of a breach of security.

Notification is not required if, after an investigation and consultation with law enforcement, it is determined that there is no reasonable likelihood of harm to customers.

Specific Content Requirements

None.

Timing

The disclosure shall be made without unreasonable delay, but not later than 90 days after becoming aware of the breach.

Any person who maintains personal information that the person does not own shall notify the owner or licensee of the information of any breach immediately following its discovery, if the personal information was, or is reasonably believed to have been, accessed by an unauthorized person.

Penalty/Private Right of Action

Failure to comply with this statute constitutes unfair trade practices for the purposes of § 42-110b, and is enforced by the Attorney General.

Other Provisions

The Connecticut Attorney General must be notified following a breach of security no later than 90 days after becoming aware of the breach.

All licensees and registrants of the Connecticut Insurance Department are required to notify the department of any information security

incident which affects any Connecticut residents as soon as the incident is identified, but no later than five calendar days after the incident is identified.

Notification pursuant to laws, rules, regulations, guidance or guidelines established by an entity's primary or functional state regulator is sufficient for compliance.

Identity theft prevention services must be provided at no cost, for a period of at least 24 months, to residents whose personal information was breached or is reasonably believed to have been breached from computerized data owned by a Connecticut business.

BakerHostetler

Delaware

Del. Code Ann. Tit. 6 § 12B-100-104 (2005); as amended (2017)

Quick Notes

- "Personal Information" is broader than the general definition.
- Notification is not triggered by only access.
- A risk of harm analysis is permitted in determining when notification is triggered.
- If notice is required to more than 500 Delaware residents, then notice to the Attorney General is required within 60 days after determination of the breach of security.
- Notice is required not later than 60 days after determination of the breach of security.
- A private cause of action is not permitted.
- There is an encryption safe harbor, unless the encryption key was exposed by the breach.
- The law does not apply to paper records.

Personal Information Definition

An individual's first name or first initial and last name plus one or more of the following data elements:

1. Social Security number.

2. Driver's license number or state-issued ID card number.

3. Account number, credit card number or debit card number.

4. A federal identification card number or a passport number.

5. A username or email address in combination with a password or security question and answer that would permit access to an online account.

6. An individual's medical history, mental or physical condition, medical treatment or diagnosis by a healthcare professional, or deoxyribonucleic acid (DNA) profile.

7. A health insurance policy number, subscriber identification number or any unique identifier used by a health insurer to identify the person.

8. Unique biometric data generated from measurements or analysis of human body characteristics for authentication purposes.

9. An individual taxpayer identification number.

Persons Covered

Any individual, corporation … limited liability company … governmental subdivision … or any other legal or commercial entity that conducts business in Delaware and owns or licenses personal information.

Any person or entity who maintains computerized data that includes personal information that the person does not own or license.

Encryption/Notification Trigger

The statute applies to unencrypted computerized data. If the unauthorized acquisition includes the encryption key and the encryption key could render that personal information readable or usable, then the statute applies to encrypted computerized data.

Standard for Triggering: The statute is triggered when there is sufficient evidence to conclude that a breach of security of computerized data has taken place. However, if after an investigation there is a determination that the breach is "unlikely to result in harm" to the affected individual(s), notice is not required.

Specific Content Requirements

None.

Timing

Notice must be made without unreasonable delay, but not later than 60 days after determination of the breach of security, unless:

1. A shorter time is required under federal law.
2. A law enforcement agency delays notice to affected individuals because it would impede a criminal investigation.
3. The covered person cannot through reasonable diligence identify certain Delaware residents whose personal information was breached within 60 days. Such person must provide notice as soon as practicable.

A person who maintains personal information that the person does not own or license shall give notice to and cooperate with the owner or licensee of the information following a breach.

Penalty/Private Right of Action

The Attorney General may bring an action in law or equity to address violations of this chapter and for other relief that may be appropriate or to recover direct economic damages resulting from a violation, or both. The provisions of this statute are not exclusive and do not relieve a person subject to this statute from compliance with all other applicable provisions of law.

Nothing in this statute may be construed to modify any right which a person may have at common law, by statute or otherwise.

Other Provisions

Covered persons must provide notice to the Delaware Attorney General's Office of any breach of security requiring notice to more than 500 Delaware residents within 60 days.

If the breach affected Social Security numbers, the covered person shall offer reasonable identity theft prevention services and, if applicable, identity theft mitigation services at no cost for a period of one year to each affected resident whose Social Security number was breached. Identity protection services are not required if it is determined harm is unlikely to result from the breach.

BakerHostetler

District of Columbia

D.C. Code § 28-3851 to 28-3853 (2007)

Quick Notes

- "Personal Information" is broader than the general definition.
- Notification is not triggered by only access.
- A risk of harm analysis is not permitted in determining when notification is triggered.
- Notice to the Attorney General or State Agency is not required.
- Notice is not required within an explicit number of days, but it must be given without unreasonable delay.
- A private cause of action is permitted.
- There is an encryption safe harbor.
- The law does not apply to paper records.

Personal Information

A person's first name or first initial and last name, or phone number, or address, in combination with one of the following:

1. Social Security number.

2. Driver's license number or District of Columbia Identification Card number.

3. Credit card number or debit card number; or any other number or code or combination of numbers or codes, such as account number, security code, access code or password, that allows access to or use of an individual's financial or credit account.

Persons Covered

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

Encryption/Notification Trigger

The acquisition of data that has been rendered secure, so as to be unusable by an unauthorized third party, is not considered a breach of the security system.

Standard for Triggering: The statute is triggered when the person or entity discovers a breach of the security system.

"Breach of the security of the system" means unauthorized acquisition of computerized or other electronic data, or any equipment or device storing such data that compromises the security, confidentiality or integrity of personal information maintained by the person or business.

Specific Content Requirements

N/A

Timing

Notice must be provided in the most expedient time possible and without unreasonable delay.

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

Any person or entity who maintains, handles or otherwise possesses computerized or other electronic data that includes personal information that the person or entity does not own shall notify the owner or licensee of the information of any breach of the security of the system, in the most expedient time possible following discovery.

Penalty/Private Right of Action

Any District of Columbia resident injured by a violation may institute a civil action to recover actual damages, the costs of the action and reasonable attorney's fees. Actual damages shall not include dignitary damages, including pain and suffering.

The Attorney General may petition the Superior Court of the District of Columbia for injunctive relief and/or restitution. The Attorney General may recover a civil penalty of $100 for each resident not provided notice, attorneys' fees for pursuing the action, and costs.

Other Provisions

N/A

BakerHostetler

Florida

Fla. Stat. Ann. § 501.171 (2014)

Quick Notes

- "Personal Information" is broader than the general definition.
- Notification is triggered by only access.
- A risk of harm analysis is permitted in determining when notification is triggered.
- If the breach affects 500 or more Florida residents, then notice to the Attorney General is required no later than 30 days after determination of the breach.
- Notice is required no later than 30 days after the determination of a breach.
- A private cause of action is not permitted.
- There is an encryption safe harbor.
- The law does not apply to paper records.

Personal Information Definition

An individual's first name or first initial and last name plus one or more of the following data elements:

1. Social Security number.

2. Driver's license number state-issued ID card number, passport number, military identification card number or other government identification number.

3. Account number, credit card number or debit card number.

4. Medical information.

5. Health insurance policy number or health insurance identification number and any unique identifier used by a health insurer to identify an individual.

A username or email address in combination with a password or a security question and answer that would permit access to an online account.

Persons Covered

A sole proprietorship, partnership, corporation, trust, estate, cooperative, association or other commercial entity that acquires, maintains, stores or uses personal information, including a governmental entity.

A third-party agent is an entity that has been contracted to maintain, store or process personal information on behalf of a covered entity or governmental entity.

Encryption/Notification Trigger

The statute only applies to unencrypted information.

Standard for Triggering: The statute is triggered upon a determination of unauthorized access of data in electronic form containing personal information.

Notice to the affected individuals is not required if, after an investigation and consultation with law enforcement, the covered entity determines the breach has not resulted and will not likely result in identity theft or any other financial harm. Such a determination must be documented in writing, submitted to the department within 30 days and maintained as a record for at least five years.

Specific Content Requirements

The notice to an individual with respect to a breach of security shall include, at a minimum:

1. The date, estimated date or estimated date range of the breach of security.

2. A description of the personal information that was, or was reasonably believed to have been, affected.

3. The covered entity's contact information to receive inquiries from affected individuals.

Timing

A covered entity shall give notice to each affected individual. Notice shall be made expediently and without unreasonable delay, but no later than 30 days after discovering, or having reason to know of, the occurrence of a breach.

Third-party agents shall notify the covered entity of a breach as soon as practicable, but no later than 10 days following the determination of a breach.

Penalty/Private Right of Action

There is no private right of action.

A violation is an "unfair or deceptive trade practice" under Florida law.

An entity that violates the provisions regarding notification is liable for a civil penalty of $1,000 per day up to 30 days following any violation, and $50,000 per 30-day period thereafter, up to a maximum total of $500,000. These penalties apply per breach and not per individual affected by the breach.

Other Provisions

If the breach affects 500 or more Florida residents, covered entities must provide written notice to the Florida Department of Legal Affairs as expediently as possible, but not later than 30 days after determination of a breach.

The notice must include:

1. A synopsis of the events surrounding the breach at the time notice is provided.

2. The number of individuals in this state who were or potentially have been affected by the breach.

3. Any services related to the breach being offered or scheduled to be offered, without charge, by the covered entity to individuals, and instructions as to how to use such services.

4. A copy of the notice sent to individuals or an explanation of the other actions taken pursuant to the statute.

5. The name, address, telephone number and email address of the employee or agent of the covered entity from whom additional information may be obtained about the breach.

BakerHostetler

Georgia

O.C.G.A. §§ 10-1-911 to 912

Quick Notes

- "Personal Information" is broader than the general definition.
- Notification is not triggered by only access.
- A risk of harm analysis is not permitted in determining when notification is triggered.
- Notice to the Attorney General or State Agency is not required, but if more than 10,000 residents must be notified at one time, the covered entity must notify all consumer reporting agencies.
- Notice is not required within an explicit number of days, but it must be made expediently and without unreasonable delay.
- A private cause of action is not permitted.
- There is an encryption safe harbor.
- The law does not apply to paper records.

Personal Information

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

1. Social Security number.

2. Driver's license or state ID card number.

3. Account number, credit card number or debit card number where the number can be used without additional identifying information, access codes or passwords.

Account passwords, personal identification numbers or other access codes.

A password and any of the data elements not in connection with the name if any of the other data elements alone would be sufficient to perform or attempt to perform identity theft against the person whose information was compromised.

Persons Covered

Any information broker or data collector that maintains computerized data, or any person or business who maintains computerized data on behalf of an information broker or data collector.

Encryption/Notification Trigger

The statute only applies to unencrypted personal information.

Standard for Triggering: The statute is triggered when a person covered by the statute becomes aware of an 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.

Specific Content Requirements

None.

Timing

Notice must be given in the most expedient time possible and without unreasonable delay, subject to the needs of law enforcement.

Any person or business that maintains computerized data on behalf of an information broker or data collector that includes personal information of individuals must give notice to the broker or collector within 24 hours following discovery if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Penalty/Private Right of Action

N/A

Other Provisions

If more than 10,000 residents must be notified at one time, the covered entity must notify, without unreasonable delay, all consumer reporting agencies.

BakerHostetler

Guam

Guam Code Ann. Tit. IX, § 48-10 (2009)

Quick Notes

- "Personal Information" is not broader than the general definition.
- Notification is not triggered by only access.
- A risk of harm analysis is not permitted in determining when notification is triggered.
- Notice to Attorney General or State Agency is not required.
- Notice is not required within an explicit number of days, but it must be given without unreasonable delay.
- A private cause of action is not permitted.
- There is an encryption safe harbor.
- The law does not apply to paper records.

Personal Information

An individual's first name or first initial with last name with one of the following identifiers:

1. Social Security number.

2. Driver's license or identification card number.

3. Account number, credit or debit card number, in combination with a linked security or access code, or password of an individual's financial account.

Persons Covered

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

An individual or entity who maintains computerized data that includes personal information that the individual or entity does not own or license.

Encryption/Notification Trigger

Does not apply to encrypted data unless the security breach involves a person with access to the encryption key and the individual or entity reasonably believes that such breach has caused or will cause identity theft or other fraud to any resident of Guam.

Standard for Triggering: An individual or entity that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach of the security of the system to any resident of Guam whose personal information was or is believed to have been accessed and acquired by an unauthorized person and that causes, or the individual or entity reasonably believes has caused or will cause, identity theft or other fraud to any resident of Guam.

An individual or entity that maintains computerized data that includes personal information that the individual or entity does not own or license shall notify the owner or licensee of the information of any breach of the security of the system if the personal information was, or if the entity reasonably believes the personal information was, accessed and acquired by an unauthorized person.

Specific Content Requirements

N/A

Timing

An individual or entity that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system made without unreasonable delay.

An individual or entity that maintains computerized data that includes personal information that the individual or entity does not own or license shall notify the owner or licensee of the information of any breach of the security of the system as soon as practicable following discovery.

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

Penalty/Private Right of Action

The Office of the Attorney General has exclusive authority to bring action and may obtain either actual damages for a violation of this chapter 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.

Other Provisions

N/A

BakerHostetler

Hawaii

Hawaii Rev. Stat. § 487N-1-4 (2006)

Quick Notes

- "Personal Information" is not broader than the general definition.
- Notification is not triggered by only access.
- A risk of harm analysis is permitted in determining when notification is triggered.
- The Office of Consumer Protection must be notified of the timing, content and distribution of the notice if the breach involves over 1,000 individuals.
- Notice is not required within an explicit number of days, but it must be made without unreasonable delay.
- A private cause of action is permitted.
- There is an encryption safe harbor.
- The law applies to electronic and paper records.

Personal Information

An individual's first name or first initial with last name combined with one or more of the following data elements, if either the name or the data elements are not encrypted:

1. Social Security number.

2. Driver's license number or Hawaii identification card number.

3. Account number, credit card number or debit card number, in combination with any access code or password that would permit access to an individual's financial account.

Persons Covered

Entities conducting business in Hawaii that may or may not own or license personal information of Hawaii residents, businesses that own or license personal information of Hawaii residents, and government agencies that collect personal information, regardless of whether the personal information is stored in computerized or paper records.

Encryption/Notification Trigger

The statute only applies to disclosure of unencrypted or unredacted information.

Standard for Triggering: The statute is triggered upon discovery or notification of a security breach.

Notification is not required if the business determines after a reasonable investigation that there is no reasonable likelihood of harm.

Specific Content Requirements

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

1. The incident in general terms.

2. The type of personal information affected.

3. The general acts of the covered entity to protect the personal information from further unauthorized access.

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

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

Timing

Notification shall be made without unreasonable delay, consistent with the needs of law enforcement and consistent with any measures

necessary to determine sufficient contact information and the scope of the breach, and to restore the reasonable integrity, security and confidentiality of the data system.

If the covered entity does not own or license the affected data, that entity must notify the owner or licensee of the personal information of any security breach immediately following discovery of the breach.

Penalty/Private Right of Action

The Attorney General or the executive director of the office of consumer protection may bring an action pursuant to this section. No such action may be brought against a government agency.

Any business that violates any provision of this chapter shall be subject to penalties of not more than $2,500 for each violation.

Any business 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 in any action brought under this section may award reasonable attorneys' fees to the prevailing party. No such action may be brought against a government agency.

The penalties provided in this section shall be cumulative to the remedies or penalties available under all other laws of this state.

Other Provisions

If over 1,000 individuals are affected, notice of the timing, content and distribution of the notice must be given to the Hawaii Office of Consumer Protection.

BakerHostetler

Idaho

Idaho Code Ann. § 28-51-104-107 (2006)

Quick Notes

- "Personal Information" is not broader than the general definition.
- Notification is not triggered by only access.
- A risk of harm analysis is permitted in determining when notification is triggered.
- If the entity is a public agency, it must notify the Attorney General within 24 hours of discovery.
- Notice is not required within an explicit number of days, but it must be made in the most expedient time possible and without unreasonable delay.
- A private cause of action is not permitted.
- There is an encryption safe harbor.
- The law does not apply to paper records.

Personal Information

An individual's first name or first initial with last name combined with one or more of the following data elements, if the name or data elements are not encrypted:

1. Social Security number.

2. Driver's license or Idaho identification card number.

3. 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.

Persons Covered

A city, county or state agency, individual or a commercial entity that conducts business in Idaho and owns or licenses data containing personal information of Idaho residents.

Encryption/Notification Trigger

The statute only applies to unencrypted personal information.

Standard for Triggering: The statute is triggered when a person covered by the statute becomes aware of the illegal acquisition of unencrypted computerized data that materially compromises the security, confidentiality or integrity of personal information.

Notice is not required if an investigation determines there is no reasonable likelihood that misuse of information about an Idaho resident has occurred or is reasonably likely to occur.

Specific Content Requirements

N/A

Timing

Notice must be made expediently and without unreasonable delay, consistent with the needs of law enforcement and with any measures necessary to determine the scope of the breach, to identify the individuals affected, and to restore the reasonable integrity of the computerized data system.

An entity that maintains data that it does not own or license shall give notice to and cooperate with the owner or licensee of the information of any discovery of a breach.

When an agency becomes aware of a breach of the security of the system, it shall, within 24 hours of such discovery, notify the office of the Idaho Attorney General.

This statute does not relieve a state agency's responsibility to report a security breach to the office of the chief information officer within the department of administration, pursuant to the information technology resource management council policies.

Penalty/Private Right of Action

The primary regulator may bring a civil action to enforce compliance with this section and enjoin an agency, individual or commercial entity from further violations.

Any agency, individual or commercial entity that intentionally fails to give notice in accordance with section 28-51-105, Idaho Code, shall be subject to a fine of not more than $25,000 per breach of the security of the system.

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

Other Provisions

Only public agencies are required to provide notice to the Idaho Attorney General, and they must do so within 24 hours.

The agency must also report a security breach to the office of the chief information officer within the department of administration, pursuant to the Information Technology Resource Management Council policies.

BakerHostetler

Illinois

815 Ill. Comp. Stat. Ann. 530/1-/30 (2006); as amended (2016)

Quick Notes

- "Personal Information" is broader than the general definition.
- Notification is not triggered by only access.
- A risk of harm analysis is not permitted in determining when notification is triggered.
- If the entity is a State Agency and more than 250 Illinois residents are affected by the breach, the entity must notify the Attorney General within 45 days or at the same time the State Agency provides notice to consumers (whichever is sooner). Entities subject to HIPAA and that provide notification to the Secretary of Health and Human Services must also provide notice to the Attorney General within 5 days of notifying HHS.
- A State Agency must notify the Attorney General within 45 days of discovery.
- A private cause of action is permitted.
- There is an encryption safe harbor.
- The law does not apply to paper records.

Personal Information

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

1. Social Security number.

2. Driver's license number or state identification card number.

3. Account number, credit card number or debit card number, in combination with any security code, access code or password required to access the account.

4. Health insurance information.

5. Medical information.

6. Biometric data.

An individual's username or email address combined with a password or security question and answer that would permit online access to an account.

Persons Covered

Any data collector that owns or licenses personal information concerning an Illinois resident and any data collector that maintains computerized data that includes personal information that the data collector does not own or license.

Encryption/Notification Trigger

The statute only applies to unencrypted data. If the encryption key was unlawfully disclosed, then the statute applies to encrypted data that the encryption key makes readable.

Standard for Triggering: The statute is triggered upon discovery or notification of an unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal information.

Data collectors or service providers that maintain or store information must cooperate with the data owner or licensor with respect to breaches of personal information in the service provider's care.

Specific Content Requirements

Notice must include contact information for credit reporting agencies and the FTC, along with a statement that the individual can obtain information from these sources about fraud alerts and security freezes.

Notice must not include information concerning the number of Illinois residents affected by the breach.

For a breach of username/email and password credentials, notice may be provided in electronic or other form directing the Illinois resident

whose personal information has been breached to promptly change his or her username or password and security question or answer, as applicable, or to take other precautionary steps.

Timing

Notification shall be made expediently and without unreasonable delay, subject to the needs of law enforcement, and consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security and confidentiality of the data system.

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

Penalty/Private Right of Action

Violations constitute an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act, and any person who suffers actual damages may bring an action under that statute.

Violations are subject to a civil penalty of not more than $100 for each individual with respect to whom personal information is disposed of in violation. A civil penalty may not exceed $50,000 for each instance of improper disposal. In addition, the Attorney General may bring an action in the circuit court to remedy a violation, seeking appropriate relief.

Other Provisions

A state agency suffering a breach affecting more than 250 Illinois residents must provide notice to the Illinois Attorney General within 45 days or at the same time the state agency provides notice to consumers (whichever is sooner). Notification to the Attorney General must include:

1. The types of personal information compromised in the breach.
2. The number of Illinois residents affected by the breach at the time of notification.
3. Any steps the state agency has taken or plans to take relating to notification of the breach to consumers.
4. The date and time frame of the breach, if known at the time notification is provided.

If the state agency is directly responsible to the governor and has a breach affecting more than 250 Illinois residents, the agency is required to notify both the Chief Information Security Officer of the Department of Innovation and Technology and the Illinois Attorney General without delay, but no later than 72 hours following discovery.

Any state agency that collects personal information and has had a breach of security of the system data or written material shall submit a report within five business days of the discovery or notification of the breach to the General Assembly listing the breaches, and outlining any corrective measures that have been taken to prevent future breaches, of the security of the system data or written material.

BakerHostetler

Indiana

Ind. Code Ann. §§ 24-4.9 et seq.; § 4-1-11 et seq. (2006); as amended (2009)

Quick Notes

- "Personal Information" is not broader than the general definition.
- Notification is not triggered by only access.
- A risk of harm analysis is permitted in determining when notification is triggered.
- The Attorney General must be notified regarding a breach.
- Notice is not required within an explicit number of days, but it must be made without unreasonable delay.
- A private cause of action is not permitted.
- There is an encryption safe harbor.
- The statute is triggered by a breach of security in paper records.

Personal Information

A Social Security number that is not encrypted or redacted; OR

An individual's first name or first initial with last name with one of the following identifiers, if the data is unencrypted:

1. Driver's license or state identification card number.

2. Account number, credit or debit card number in combination with a security code, password or access code that would permit access to the person's account.

Persons Covered

Businesses and state agencies that own or license computerized data that includes personal information, or a person who maintains computerized data.

Encryption/Notification Trigger

The statute does not apply to encrypted information, provided that the unauthorized recipient of the information does not also get an encryption key.

Standard for Triggering: The statute is triggered upon discovery or notification of an unauthorized acquisition of computerized data or computerized data that has been transferred to another medium, including paper, microfilm or a similar media, even if the transferred data are no longer in a computerized format.

Disclosure is required by the persons/businesses if the database owner knows or should know that the unauthorized acquisition could result in identity deception, identity theft or fraud affecting the Indiana resident.

Disclosure is required by a state agency if personal information was or is reasonably believed to have been acquired by an unauthorized person.

Specific Content Requirements

None.

Timing

Persons/Businesses: A person required to make a disclosure or notification under this chapter shall make the disclosure or notification without unreasonable delay. A delay is reasonable if the delay is (1) necessary to restore the integrity of the computer system, (2) necessary to discover the scope of the breach or (3) in response to a request from the Attorney General or a law enforcement agency to delay disclosure because disclosure will:

a. Impede a criminal or civil investigation.

b. Jeopardize national security.

State Agencies: Notice must be made without unreasonable delay, consistent with:

1. Legitimate needs of law enforcement.
2. Any measures necessary to determine the scope of the breach.
3. Any measures necessary to restore the reasonable integrity of the data system.

An entity that maintains data containing personal information but does not own or license the personal information shall notify the owner of the personal information if the entity discovers that personal information was or may have been acquired by an unauthorized person.

If delay in notification is no longer necessary to restore the integrity of the computer system, or the Attorney General or law enforcement notified the person that delay will no longer impede an investigation or jeopardize national security, then notification must be made “as soon as possible.”

Penalty/Private Right of Action

A person who is required to make a disclosure or notification in accordance with IC 24-4.9-3 and who fails to comply with any provision of this article commits a deceptive act that is actionable only by the Attorney General under this chapter.

A failure to make a required disclosure or notification in connection with a related series of breaches of the security of data constitutes one deceptive act.

The Attorney General may bring an action under this chapter to obtain any or all of the following:

1. An injunction to enjoin future violations of IC 24-4.9-3.
2. A civil penalty of not more than $150,000 per deceptive act.
3. The Attorney General’s reasonable costs in:
    a. The investigation of the deceptive act.
    b. Maintaining the action.

Other Provisions

If a database owner is required to notify affected individuals, the database owner must also disclose the breach to the Attorney General.

BakerHostetler

Iowa

Iowa Code Ann. §§ 715C.1 et seq. (2008); as amended (2014)

Quick Notes

- "Personal Information" is broader than the general definition.
- Notification is not triggered by only access.
- A risk of harm analysis is permitted in determining when notification is triggered.
- If 500 or more Iowa residents must be notified, written notification must be provided to the director of the Consumer Protection Division of the Iowa Attorney General's Office within five business days of notifying any Iowa residents regarding the breach.
- Notice is not required within an explicit number of days, but it must be made expediently and without unreasonable delay.
- A private cause of action is not permitted.
- There is an encryption safe harbor.
- The statute is triggered by a breach of security in paper records.

Personal Information

An individual's first name or first initial with last name with one of the following identifiers, if the data is unencrypted:

1. Social Security number.

2. Driver's license or identification card number.

3. Account number, credit or debit card number, security or access code, or password of an individual's financial account.

4. A 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.

5. Unique biometric data, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data.

Persons Covered

Any person who owns or licenses computerized data that includes a consumer's personal information that is used in the course of the person's business, vocation, occupation or volunteer activities, or who maintains or otherwise possesses personal information on behalf of another person.

Encryption/Notification Trigger

The statute does not cover personal information if it is "encrypted, redacted, or otherwise altered in such a manner that the name or data elements are unreadable" unless the keys to unencrypt, unredact or otherwise read the data have been obtained through a breach of security.

Standard for Triggering: The statute is triggered upon discovery of a breach of security or upon notification of a breach of security by a data licensee.

Notification is not required if, after an investigation and consultation with law enforcement, there is a determination that no reasonable likelihood of financial harm will result to the affected individuals. This determination must be documented in writing and maintained for five years.

Specific Content Requirements

Notice must include, at a minimum, all of the following:

(a) A description of the breach of security.

(b) The approximate date of the breach of security.

(c) The type of personal information obtained as a result of the breach of security.

(d) Contact information for consumer reporting agencies.

(e) Advice to the consumer to report suspected incidents of identity theft to local law enforcement or the Attorney General.

Timing

The consumer notification must be made expediently and without unreasonable delay, consistent with the needs of law enforcement, and consistent with any measures necessary to sufficiently determine contact information for the affected consumers, determine the scope of the breach, and restore the reasonable integrity, security and confidentiality of the data.

Penalty/Private Right of Action

Violations are an unlawful practice under Iowa's Consumer Fraud Statute. Consequences include damages for injury and a fine of up to $40,000 per violation.

Other Provisions

For a breach of security requiring notification of 500 or more Iowa residents pursuant to Iowa law, written notification must be provided to the director of the consumer protection division of the Iowa Attorney General within five business days of notifying any Iowa residents regarding the breach.

BakerHostetler

Kansas

Kan. Stat. Ann. §§ 50-7a01 & 7a02 (2006)

Quick Notes

- "Personal Information" is not broader than the general definition.
- Notification is not triggered by only access.
- A risk of harm analysis is permitted in determining when notification is triggered.
- Notice to the Attorney General or State Agency is not required.
- Notice is not required within an explicit number of days, but it must be made expediently and without unreasonable delay.
- A private cause of action is not permitted.
- There is an encryption safe harbor.
- The law does not apply to paper records.

Personal Information

An individual's first name or first initial with last name with one of the following identifiers, if the data is unencrypted:

1. Social Security number.

2. Driver's license or identification card number.

3. Financial account number, or credit or debit card number, alone or in combination with any required security code access code, or password that would permit access to an individual's financial account.

Persons Covered

A person who conducts business in this state, or a government, governmental subdivision or agency that owns or licenses computerized data that includes personal information, or an individual or a commercial entity who maintains computerized data that includes personal information that the individual or the commercial entity does not own or license.

Encryption/Notification Trigger

The statute only applies to unencrypted or unredacted information.

Standard for Triggering: The statute is triggered when a person becomes aware of any breach of the security of the system.

A covered entity, once it becomes aware of a breach, must conduct an investigation to determine the likelihood that the personal information has been or will be misused. Notice is required to the affected individuals if the investigation determines that the misuse of information has occurred or is reasonably likely to occur.

Specific Content Requirements

N/A

Timing

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

An entity that maintains computerized data that includes personal information that the entity does not own or license shall give notice to the owner or licensee of the information of any breach of data following discovery of a breach, if the personal information was, or is reasonably believed to have been, accessed and acquired by an unauthorized person.

Penalty/Private Right of Action

For violations of this section, except as to insurance companies licensed to do business in this state, the Attorney General is empowered to bring an action in law or equity to address violations of this section and for other relief that may be appropriate.

For violations of this section by an insurance company licensed to do business in this state, the insurance commissioner shall have the sole authority to enforce the provisions of this section.

Other Provisions

For a breach requiring notice to more than 1,000 Kansas residents at one time, the covered entity must also notify, without unreasonable delay, the major consumer reporting agencies of the timing, distribution and content of the notices.

BakerHostetler

Kentucky

Ky. Rev. Stat. Chapter 365 (as amended by H.B. 232 on April 10, 2014)

Quick Notes

- "Personal Information" is not broader than the general definition.
- Notification is not triggered by only access.
- A risk of harm analysis is permitted in determining when notification is triggered.
- Notice to the Attorney General or State Agency is not required, but if more than 1,000 persons must be notified at one time, then the information holder must notify all consumer reporting agencies.
- Notice is not required within an explicit number of days, but it must be made expediently and without unreasonable delay.
- A private cause of action is not permitted.
- There is an encryption safe harbor.
- The law does not apply to paper records.

Personal Information (i.e., "Personally Identifiable Information")

An individual's first name or first initial with last name with one of the following identifiers, if the data is unencrypted:

1. Social Security number.

2. Driver's license or identification card number.

3. Account number, credit or debit card number, security or access code, or password of an individual's financial account.

Persons Covered

Any information holder, including an information holder that maintains computerized data that includes personally identifiable information that the information holder does not own.

An "information holder" is any person or business who conducts business in Kentucky.

Encryption/Notification Trigger

The statute only applies to unencrypted and unredacted computerized data.

Standard for Triggering: The statute is triggered when an information holder discovers or is notified of any unauthorized acquisition of unencrypted and unredacted computerized data that compromises the security, confidentiality or integrity of personally identifiable information maintained by the information holder.

Specific Content Requirements

N/A

Timing

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

If the information holder does not own or license the computerized data, including personally identifiable information, he or she must notify the owner or licensee of the information of any breach as soon as practicable following discovery if the personally identifiable information was, or is reasonably believed to have been, acquired by an unauthorized person.

Penalty/Private Right of Action

N/A

Other Provisions

If more than 1,000 persons must be notified at one time, the information holder must notify, without unreasonable delay, all consumer reporting agencies and credit bureaus that compile and maintain files on consumers on a nationwide basis.

BakerHostetler

Louisiana

La. Rev. Stat. § 51:3071-3077 (2005); L.A.C. 16:III.701

Quick Notes

- "Personal Information" is broader than the general definition.
- Notification is not triggered by only access.
- A risk of harm analysis is permitted in determining when notification is triggered.
- Notice to the Attorney General is required when notice must be given to Louisiana citizens, and is required within 10 days of the distribution of notice to Louisiana citizens.
- Notice is required in the most expedient time possible and without delay, but not later than sixty days.
- A private cause of action is permitted.
- There is an encryption safe harbor.
- The law does not apply to paper records.

Personal Information

An individual's first name or first initial with last name with one of the following identifiers, if the data is unencrypted:

1. Social Security number.

2. Driver's license or identification card number.

3. Account number, credit or debit card number, security or access code, or password of an individual's financial account.

4. Passport number.

5. Biometric data.

Persons Covered

Any individual, corporation, partnership, sole proprietorship, joint stock company, joint venture, or any other legal entity that owns or licenses computerized data that includes personal information, or any agency that owns or licenses computerized data that includes personal information, and discovers a breach in the security of the system containing personal information that is reasonably believed to be acquired by an unauthorized person.

Encryption/Notification Trigger

Notification requirement only applies where the personal information was not encrypted or redacted.

Standard for Triggering: The statute is triggered upon discovery of a breach of the security of the system containing personal information.

Notification is not required if after reasonable investigation the person or business determines that there is no reasonable likelihood of harm to Louisiana residents. The covered entity must maintain a copy of the written determination of such, along with any supporting documentation, for five years after the date the breach was discovered.

Specific Content Requirements

N/A

Timing

Notification must be provided in the most expedient time possible and without unreasonable delay but not later than sixty days from the discovery of the breach. Notification may be delayed if law enforcement determines that notification would impede a criminal investigation.

Any individual, corporation, partnership, sole proprietorship, joint stock company, joint venture or any other legal entity that maintains computerized data that includes personal information that the agency or person does not own shall notify the owner or licensee of the

information if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person through a breach of security of the system containing such data, following discovery by the agency or person of a breach of the security system.

Penalty/Private Right of Action

A civil action may be brought to recover actual damages resulting from the failure to disclose in a timely manner to a person that there was a breach of the security system resulting in disclosure of the person's personal information. Failure to provide timely notice may be punishable by a fine not to exceed $5,000 per violation. Notice to the Consumer Protection Section of the Attorney General's Office shall be timely if received within 10 days of distribution of notice to Louisiana citizens. Each day notice is not received by the Attorney General shall be deemed a separate violation.

Other Provisions

The Consumer Protection Section of the Louisiana Attorney General's Office must be notified regarding a breach within 10 days of distribution of notice to affected individuals. Notice shall include the names of all Louisiana citizens affected.

A violation of the statute constitutes an unfair act or practice under R.S. 51:1405(A).

BakerHostetler

Maine

Maine Rev. Stat. Ann. Tit. 10, § 1346-49 (2005)

Quick Notes

- "Personal Information" is broader than the general definition.
- Notification is not triggered by only access.
- A risk of harm analysis is permitted in determining when notification is triggered.
- Notice to the Attorney General, or to the Department of Professional and Financial Regulation if the entity is governed by that body, must be given regarding a breach.
- Notice is required within seven business days after a law enforcement agency determines that the notification will not compromise a criminal investigation.
- A private cause of action is not permitted.
- There is an encryption safe harbor.
- The law does not apply to paper records.

Personal Information

An individual's first name or first initial with last name with one of the following identifiers, if the data is unencrypted:

1. Social Security number.

2. Driver's license or identification card number.

3. Account number, credit or debit card number, security or access code, or password of an individual's financial account.

4. Account passwords or personal identification numbers or other access codes.

5. Any single data element from the definition of PI when not in connection with the individual's first name or first initial and last name, if the information is compromised, would be sufficient to permit a person to fraudulently assume or attempt to assume the identity of the person whose information was compromised.

Persons Covered

Information brokers and other persons, as well as third-party entities, who maintain computerized data that includes personal information.

"Information broker" means a person who engages in collecting, assembling and evaluating … information concerning individuals for the primary purpose of furnishing personal information to nonaffiliated third parties. The term does not include a governmental agency whose records are maintained primarily for traffic safety, law enforcement or licensing purposes.

Encryption/Notification Trigger

The statute only applies to disclosure of information that is not encrypted.

Standard for Triggering: The statute is triggered when a person covered by the statute becomes aware of the unauthorized acquisition, release or use of personal information.

Notification is not required if it is determined, after an investigation, there is not a reasonable likelihood that the personal information has been or will be misused.

Specific Content Requirements

N/A

Timing

Notice must be made expediently and without unreasonable delay, subject to law enforcement and any measures necessary to secure the integrity of the data system.

Notification may be delayed for no longer than seven business days after a law enforcement agency determines that the notification will not compromise a criminal investigation.

A third-party entity that maintains computerized data that includes personal information that the third-party entity does not own shall notify the owner of the information of any breach if the data was believed to be acquired by an unauthorized person.

Penalty/Private Right of Action

A person who violates this chapter commits a civil violation and is subject to one or more of the following: a fine of not more than $500 per violation, up to a maximum of $2,500 for each day the person is in violation of this chapter, and enjoinment from further violations of this chapter.

The appropriate state regulators within the Department of Professional and Financial Regulation shall enforce this chapter for any person who is licensed or regulated by those regulators. The Attorney General shall enforce this statute for all other persons.

Other Provisions

Notice must be provided to the Attorney General, or to the Department of Professional and Financial Regulation if the entity is governed by that body.

BakerHostetler

Maryland

Md. Code Ann., Com. Law § 14-3501-3508 (2007); as amended (2017)

Quick Notes

- "Personal Information" is broader than the general definition.
- Notification is not triggered by only access.
- A risk of harm analysis is permitted in determining when notification is triggered.
- The Attorney General must be notified prior to notification of individuals.
- Notice is required as soon as practicable, but not later than 45 days after the business discovers or is notified of the breach.
- A private cause of action is permitted under Title 13 of the Maryland Code, the Unfair and Deceptive Trade Practices Act.
- There is an encryption safe harbor.
- The law does not apply to paper records.

Personal Information

An individual's first name or first initial with last name with one of the following identifiers, if the data is unencrypted:

1. Social Security number, individual taxpayer identification number, passport number or other federal government-issued identification number

2. Driver's license or state identification card number.

3. Account number, credit or debit card number, security or access code, or password of an individual's financial account.

4. Health information, including information about an individual's mental health

5. A health insurance policy or certificate number, or health insurance subscriber identification number, in combination with a unique identifier user by an insurer or self-insured employer that permits access to an individual's health information.

6. An individual's biometric data.

7. A username and email address in combination with a password or security question and answer that permits access to an individual's email account.

Persons Covered

A business that owns or licenses computerized data that includes personal information of an individual residing in the state; a business that maintains computerized data that includes personal information that the business does not own or license.

Encryption/Notification Trigger

The statute only applies to information that is not encrypted, redacted or otherwise protected by another security method.

Standard for Triggering: The statute is triggered when a covered entity discovers or is notified of a breach of the security of the system.

Notification is not required if, after an investigation, the entity determines that the personal information of the individual was not and will not be misused as a result of the breach. A record of this determination shall be maintained for three years after it is made.

Specific Content Requirements

The notification must include (1) the types of personal information affected, (2) contact information for the business making the notification, (3) toll-free telephone numbers and addresses for the major consumer reporting agencies and (4) the toll-free numbers, addresses and website addresses for the FTC and Office of the

Attorney General, and a statement that an affected individual can obtain information from these sources about steps he or she can take to avoid identity theft.

If the breach permits access to an individual's email account, the business may comply with the notification requirement by providing the notification in electronic or other form, and directing the affected individual to change his or her password or take other appropriate steps to protect the email account.

Timing

Notification shall be given as soon as reasonably practicable, but not later than 45 days after the business discovers or is notified of the breach of the security of the system, subject to the needs of law enforcement and any measures necessary to identify affected individuals or restore the integrity of the data system.

If law enforcement delays notification, notification must be made as soon as practicable, but not later than 30 days after the law agency determines it is safe to make notification.

An entity that maintains data, including personal information that the entity does not own or license, shall notify the owner or licensee of the personal information as soon as practicable if the information is likely to be misused as a result of the breach. A third-party entity shall share with the owner or licensee information relative to the breach.

Penalty/Private Right of Action

A violation of this subtitle is:

(1) An unfair or deceptive trade practice within the meaning of the Maryland Consumer Protection Act.

(2) Subject to the enforcement and penalty provisions contained in the Maryland Consumer Protection Act.

Other Provisions

Maryland requires businesses to follow reasonable procedures to guard against data breaches:

When a business is destroying a customer's records that contain personal information of the customer, the business shall take reasonable steps to protect against unauthorized access to or use of the personal information, taking into account (1) the sensitivity of the records, (2) the nature and size of the business and its operations, (3) the costs and benefits of different destruction methods and (4) available technology.

Notification to the Attorney General is required prior to notifying individuals.

A business required to notify 1,000 or more residents must also notify each consumer reporting agency that compiles and maintains files on consumers on a nationwide basis as to the timing, distribution, and content of the notices.

BakerHostetler

Massachusetts

Mass. Gen. Law Ann. Ch. 93H, §§ 1-6 (2007); Mass. Gen. Laws Ann. Ch. 93A, § 4 (2007)

Quick Notes

- "Personal Information" is broader than the general definition.
- Notification is not triggered by only access.
- A risk of harm analysis is permitted in determining when notification is triggered.
- The Attorney General and the director of consumer affairs and business regulation must be notified regarding a breach.
- Notice is required within seven business days after a law enforcement agency determines that the notification will not compromise a criminal investigation.
- A private cause of action is permitted under Chapter 93A, which allows for certain instances of treble damages.
- There is an encryption safe harbor.
- The law applies to electronic and paper records.

Personal Information

An individual's first name or first initial with last name with one of the following identifiers, if the data is unencrypted:

1. Social Security number.

2. Driver's license or identification card number.

3. Financial account information with or without password or security code information. This includes non-electronic personal information.

Persons Covered

A person or agency who maintains, stores, owns or licenses personal information about a resident of the commonwealth, and who knows or has reason to know of a breach of security or who knows or has reason to know that the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose.

Encryption/Notification Trigger

The statute does not apply to encrypted electronic data unless it includes the confidential process or key.

Standard for Triggering: The statute is triggered when the person or agency knows or has reason to know: (1) of a breach of security, defined as the unauthorized acquisition or use of unencrypted data or encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information and creates a substantial risk of identity theft of fraud against a resident; OR (2) that the personal information of a resident was acquired or used by an unauthorized person or used for an unauthorized purpose.

The breach must create a substantial risk of identity theft or fraud against a resident of the commonwealth or when the person or agency knows or has reason to know that the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose.

Specific Content Requirements

Notice to be provided to Massachusetts residents shall include (1) the consumer's right to obtain a police report, (2) how a consumer requests a security freeze and the necessary information to be provided when requesting a security freeze and (3) any fees required to be paid to any of the consumer reporting agencies.The contents of notification shall not include the nature of the breach, or unauthorized acquisition or use, or the number of residents affected by said breach, or unauthorized access or use.

Notice provided to the Attorney General, the director of consumer affairs and business regulation, and consumer reporting agencies or state agencies, if any, shall include (1) the nature of the breach of security or unauthorized acquisition or use, (2) the number of residents of Massachusetts affected by such incident at the time of notification and (3) any steps the entity has taken or plans to take relating to the incident.

Timing

Notice must be given as soon as practicable without unreasonable delay.

A person or agency that maintains or stores, but does not own or license, data that includes personal information about a resident of Massachusetts, shall provide notice, as soon as practicable and without unreasonable delay, when such entity knows of a breach or has reason to know that the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose.

Penalty/Private Right of Action

The Attorney General may bring an action pursuant to Section 4 of Chapter 93A against a person or otherwise to remedy violations of this chapter and for other relief that may be appropriate. Mass. Gen. Laws Ann. Ch 93A, § 4 permits the Attorney General to bring an action in the commonwealth's name. The Attorney General may seek injunctive relief, a $5,000 penalty for each violation, and reasonable costs and attorneys' fees.

Other Provisions

Notification must be made to the Attorney General and the director of consumer affairs and business regulation. Upon receipt of notice, the director of consumer affairs and business regulation will identify any relevant consumer reporting agency or state agency that needs to be notified to the notifying party.

BakerHostetler

Michigan

Mich. Comp. Laws Ann. §§ 445.63, 445.65, 445.72 (2006)

Quick Notes

- "Personal Information" is not broader than the general definition.
- Notification is not triggered by only access.
- A risk of harm analysis is permitted in determining when notification is triggered.
- Notice to the Attorney General or State Agency is not required.
- Notice is not required within an explicit number of days, but it must be made without unreasonable delay.
- A private cause of action is not permitted.
- There is an encryption safe harbor.
- The law does not apply to paper records.

Personal Information

An individual's first name or first initial with last name with one of the following identifiers:

1. Social Security number.

2. Driver's license or identification card number.

3. Account number, credit or debit card number, security or access code, or password of an individual's financial account.

Persons Covered

A person or agency who owns or licenses data included in a database who discovers a security breach, or receives notice of a security breach; a person or agency who maintains a database that includes data that the person or agency does not own or license, and who discovers a breach of the security of the database.

Encryption/Notification Trigger

A person or agency does not have to give notice if the resident's data was encrypted or redacted, and the person gaining unauthorized access did not have the encryption key.

Standard for Triggering: The statute is triggered upon discovery or notification of a security breach.

The person or agency does not have to provide notice if the person or agency determines that the security breach has not or is not likely to cause substantial loss or injury to, or result in identity theft with respect to, one or more residents of Michigan.

Specific Content Requirements

The notice must include:

1. A description of the breach in general terms.

2. A description of the personal information subject to unauthorized access or use.

3. If applicable, a description of what the covered entity has done to protect data from further security breaches.

4. A telephone number where the recipient may obtain assistance or additional information.

5. A reminder of the need to remain vigilant for incidents of fraud or identity theft.

Timing

A person or agency shall provide any notice required under this section without unreasonable delay, subject to law enforcement and any measures necessary to secure the integrity of the data system.

An entity that maintains data that the entity does not own or license shall provide a notice to the owner or licensor of the information if there has been a security breach that is likely to cause substantial loss or injury to, or result in identity theft with respect to, one or more residents of Michigan.

Penalty/Private Right of Action

A person who knowingly violates this section may be ordered to pay a civil fine of not more than $250 for each failure to provide notice. Civil fines for multiple violations shall not exceed $750,000. The Attorney General or a prosecuting attorney may bring an action to recover a civil fine.

A person who provides notice of a security breach when a security breach has not occurred, with the intent to defraud, is guilty of a misdemeanor punishable by imprisonment for not more than 93 days or a fine of not more than $250 for each violation, or both.

Other Provisions

N/A

BakerHostetler

Minnesota

Minn. Stat. Ann. §§ 325E.61, 8.31 (2005); as amended (2007)

Quick Notes

- "Personal Information" is not broader than the general definition.
- Notification is not triggered by only access.
- A risk of harm analysis is not permitted in determining when notification is triggered.
- If the breach affects over 500 people, consumer reporting agencies must be notified within 48 hours.
- Notice is not required within an explicit number of days, but it must be made expediently and without unreasonable delay.
- A private cause of action is not permitted.
- There is an encryption safe harbor.
- The law does not apply to paper records.

Personal Information

An individual's first name or first initial with last name with one of the following identifiers:

1. Social Security number.

2. Driver's license or identification card number.

3. Account number, credit or debit card number, security or access code, or password of an individual's financial account.

Persons Covered

Any person or business who conducts business in the state of Minnesota, and who owns or licenses data that includes personal information, and discovers a breach of the security of the data. Any person or business who maintains data that includes personal information that the person or business does not own, and who discovers a breach of the security of the data.

Encryption/Notification Trigger

Personal information does not include encrypted data or data that is otherwise unreadable.

Standard for Triggering: The statute is triggered upon discovery or notification of a breach of the security of the system.

Specific Content Requirements

N/A

Timing

Notification must be made expediently and without unreasonable delay, subject to law enforcement or any measures necessary to determine the scope of the breach, identify the individuals affected and restore the reasonable integrity of the data system.

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

Penalty/Private Right of Action

The Attorney General shall enforce this section by seeking injunctive relief and/or a civil penalty for the state not to exceed $25,000.

Other Provisions

For a breach affecting over 500 people (1,000 for state agencies), consumer reporting agencies must be notified within 48 hours. When notifying a consumer reporting agency, a person or business must include the timing, distribution and content of the notices being sent to the Minnesota residents.

This section does not apply to any “financial institution” as defined by United States Code, title 15, section 6809(3).

BakerHostetler

Mississippi

Miss. Code Ann. § 75-24-29 (2010)

Quick Notes

- "Personal Information" is not broader than the general definition.
- Notification is not triggered by only access.
- A risk of harm analysis is permitted in determining when notification is triggered.
- Notice to the Attorney General or a State Agency is not required.
- Notice is not required within an explicit number of days, but it must be made without unreasonable delay.
- A private cause of action is not permitted.
- There is an encryption safe harbor.
- The law does not apply to paper records.

Personal Information

An individual's first name or first initial with last name with one of the following identifiers:

1. Social Security number.

2. Driver's license or identification card number.

3. Account number, credit or debit card number, security or access code, or password of an individual's financial account.

Persons Covered

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

Encryption/Notification Trigger

The statute does not apply to encrypted data or data made unusable or unreadable by another method or technology.

Standard for Triggering: The statute is triggered by any breach of security.

Notification is not required if, after an appropriate investigation, the person reasonably determines that the breach will not likely result in harm to the affected individuals.

Specific Content Requirements

N/A

Timing

If required, disclosure must be made without unreasonable delay subject to the needs of law enforcement and to the completion of an investigation by the person to determine the nature and scope of the incident, to identify the affected individuals or to restore the reasonable integrity of the data system.

A person who maintains computerized data that includes personal information that the person does not own or license shall notify the owner or licensee of the information of any breach of security as soon as practical following its discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person for fraudulent purposes.

Penalty/Private Right of Action

Failure to comply with the requirements of this section shall constitute an unfair trade practice and shall be enforced by the Attorney General; however, nothing in this section may be construed to create a private right of action.

Other Provisions

N/A

BakerHostetler

Missouri

Mo. Rev. Stat. § 407.1500 (2009)

Quick Notes

- "Personal Information" is broader than the general definition.
- Notification is not triggered by only access.
- A risk of harm analysis is permitted in determining when notification is triggered.
- If 1,000 or more persons are affected, then the Attorney General must be notified regarding the timing, distribution and content of notice to individuals.
- Notice is not required within an explicit number of days, but it must be made without unreasonable delay.
- A private cause of action is not permitted.
- There is an encryption safe harbor.
- The law does not apply to paper records.

Personal Information

An individual's first name or first initial with last name with one of the following identifiers:

1. Social Security number.

2. Driver's license or identification card number.

3. Account number, credit or debit card number, security or access code, or password of an individual's financial account.

4. A unique electronic identifier or routing code in combination with a required security code, access code or password that would permit access to an individual's financial account.

5. Medical information, such as an individual's medical history, mental or physical condition, treatment or diagnosis.

6. Health insurance policy number, subscriber ID number and any other unique identifier used by a health insurer.

Persons Covered

Any person that owns or licenses personal information of residents of Missouri or any person that conducts business in Missouri that owns or licenses personal information in any form of a resident of Missouri, or Any person that maintains or possesses records or data containing personal information of residents of Missouri that the person does not own or license, or any person that conducts business in Missouri that the person does not own or license.

Encryption/Notification Trigger

Personal information does not include encrypted data or information that is redacted, altered or truncated such that no more than five digits of a Social Security number, or the last four digits of a driver's license number, state identification card number or account number, is accessible as part of the personal information.

Standard for Triggering: The statute is triggered upon discovery or notification of a breach of security.

Notification is not required if, after an investigation, the person determines that a risk of identity theft or other fraud to any consumer is not reasonably likely to occur as a result of the breach. Such a determination shall be documented in writing and the documentation shall be maintained for five years.

Specific Content Requirements

The notice shall, at minimum, include a description of the following: (a) the incident in general terms, (b) the type of personal information that was obtained as a result of the breach of security, (c) a telephone

number that the affected consumer may call for further information and assistance, if one exists, (d) contact information for consumer reporting agencies and (e) advice that directs the affected consumer to remain vigilant by reviewing account statements and monitoring free credit reports.

Timing

For an owner of personal information, the disclosure notification shall be (a) made without unreasonable delay, (b) consistent with the legitimate needs of law enforcement and (c) consistent with any measures necessary to determine sufficient contact information and determine the scope of the breach, and to restore the reasonable integrity, security and confidentiality of the data system.

If the covered entity does not own or license the affected information, notice must be made to the owner or licensee of the information of any breach of security immediately following discovery of the breach, consistent with the legitimate needs of law enforcement.

Penalty/Private Right of Action

The Attorney General shall have exclusive authority to bring an action to obtain actual damages for a willful and knowing violation of this section, 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.

Other Provisions

If 1,000 or more persons are affected, both the Attorney General and consumer reporting agencies must be notified of the timing, distribution and content of notice sent to affected individuals.

BakerHostetler

Montana

Mont. Code Ann. §§ 30-14-1701 - 02 & 1704 (2005); as amended (2015)

Quick Notes

- "Personal Information" is broader than the general definition.
- Notification is not triggered by only access.
- A risk of harm analysis is permitted in determining when notification is triggered.
- Any covered entity required to make notification must also simultaneously submit an electronic copy of the notification, and a statement providing the date and method of distribution of the notification, to the Montana Attorney General's Consumer Protection Office.
- Notice is not required within an explicit number of days, but it must be made without unreasonable delay.
- A private cause of action is not permitted.
- There is an encryption safe harbor.
- The law does not apply to paper records.

Personal Information

An individual's first name or first initial with last name with one of the following identifiers:

1. Social Security number.

2. Driver's license or identification card number.

3. Account number, credit or debit card number, security or access code, or password of an individual's financial account.

4. Medical record information as it relates to an individual's physical or mental condition, medical history, medical claims history, or medical treatment, and is obtained from a medical professional or medical care institution, from the individual, or from the individual's spouse, parent or legal guardian.

5. Taxpayer identification number.

6. An identity protection personal identification number issued by the United States Internal Revenue Service.

Persons Covered

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

Encryption/Notification Trigger

The statute only applies to unencrypted information.

Standard for Triggering: The statute is triggered upon discovery or notification of a breach of security of the data system, defined as unauthorized acquisition of computerized data that both materially compromises the security, confidentiality, or integrity of personal information and causes, or is reasonably believed to cause, loss or injury to a Montana resident.

Notification is not required if the unauthorized access of the information causes, or is reasonably to cause loss, or injury to a Montana resident.

Specific Content Requirements

N/A

Timing

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

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

A state agency that maintains computerized data containing personal information in the data system must make reasonable efforts to notify any person whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person.

Penalty/Private Right of Action

Whenever the Montana Attorney General has reason to believe that a person has violated this part and that proceeding would be in the public interest, the department may bring an action in the name of the state against the person to restrain by temporary or permanent injunction, or temporary restraining order, the use of the unlawful method, act or practice, upon giving appropriate notice to that person pursuant to 30-14-111(2). A violation of this part is a violation of 30-14-103, and the penalties for a violation of this part are as provided in 30-14-142, including a civil fine of not more than $10,000 for each violation.

Other Provisions

Any person, business or state agency required to make a notification must also simultaneously submit an electronic copy of the notification and a statement providing the date and method of distribution of the notification to the Montana Attorney General's Consumer Protection Office, excluding any information that personally identifies any individual who is entitled to receive notification. If notification is made to more than one individual, the notification must indicate the number of individuals in the state who received notification.

BakerHostetler

Nebraska

Neb. Rev. Stat. §§ 87-802 to -806 (2006); as amended (2016)

Quick Notes

- "Personal Information" is broader than the general definition.
- Notification is not triggered by only access.
- A risk of harm analysis is permitted in determining when notification is triggered.
- If a covered entity must provide notice to a Nebraska resident, notice must be provided, not later than the time when notice is provided to the Nebraska resident(s), to the Nebraska Attorney General's Office.
- Notice is not required within an explicit number of days, but it must be made without unreasonable delay.
- A private cause of action is not permitted.
- There is an encryption safe harbor.
- The law does not apply to paper records.

Personal Information

An individual's first name or first initial with last name with one of the following identifiers:

1. Social Security number.

2. Driver's license or identification card number.

3. Account number, credit or debit card number, security or access code, or password of an individual's financial account.

4. A unique identification number or routing code, in combination with any required security code, access code or password.

5. Unique biometric data, such as fingerprint, voiceprint, or retina or iris image, or other unique physical representation.

A username or email address, in combination with a password or security question and answer that would permit access to an online account.

Persons Covered

An individual or a commercial entity who conducts business in Nebraska and who owns or licenses computerized data that includes personal information about a resident of Nebraska; an individual or commercial entity who maintains computerized data that includes personal information that the individual or commercial entity does not own or license.

Encryption/Notification Trigger

Notice is not required if data is encrypted or redacted. Personal information is not considered to be encrypted if the encryption key or process is reasonably believed to have been acquired during the breach.

Standard for Triggering: The statute is triggered when a covered person becomes aware of a breach of the security of the system and conducts a reasonable and prompt investigation, in good faith, to determine the likelihood that personal information has been or will be used for an unauthorized purpose.

The covered entity shall conduct a reasonable and prompt investigation in good faith. If the investigation determines that the use of information about a Nebraska resident for an unauthorized purpose has occurred or is reasonably likely to occur, the individual or commercial entity shall give notice to the affected Nebraska resident.

Specific Content Requirements

An individual or commercial entity that maintains the data shall provide the owner or licensee of the data information relevant to the breach,

not including information proprietary to the individual or commercial entity.

Timing

Notice to residents must be made as soon as possible without unreasonable delay, subject to law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system.

A covered entity that maintains data that it does not own or license shall give notice, and cooperate with the owner or licensee of the data, when it becomes aware of a breach, if use of personal information about a Nebraska resident for an unauthorized purpose occurred or is reasonably likely to occur.

Penalty/Private Right of Action

The Attorney General may issue subpoenas and seek and recover direct economic damages for each affected Nebraska resident injured by a violation of this act.

Other Provisions

An individual or commercial entity required to provide notice of a breach of security of the system to a Nebraska resident(s) must also, not later than the time when notice is provided to the Nebraska resident(s), provide notice of the breach of security of the system to the Nebraska Attorney General’s Office.

BakerHostetler

Nevada

Nev. Rev. Stat. §§ 603A.010-.920 (2005); as amended (2007, 2015); Nev. Rev. Stat. § 603A.210 (2005); as amended Nev. Rev. Stat. § 603A.215

Quick Notes

- "Personal Information" is broader than the general definition.
- Notification is not triggered by only access.
- A risk of harm analysis is permitted in determining when notification is triggered.
- Notice to the Attorney General or State Agency is not required.
- Notice is not required within an explicit number of days, but it must be made without unreasonable delay.
- A private cause of action is permitted.
- There is an encryption safe harbor.
- The law does not apply to paper records.

Personal Information

An individual's first name or first initial with last name with one of the following identifiers:

1. Social Security number.

2. Driver's license or identification card number.

3. Account number, credit or debit card number, security or access code, or password of an individual's financial account.

4. Medical identification number, or health insurance identification number.

5. A username, unique identifier or electronic mail address in combination with a password, access code, or security question and answer that would permit access to an online account.

This definition excludes the last four digits of a Social Security number, the last four digits of a driver's license number, the last four digits of a driver authorization card number, the last four digits of an identification card number, and publicly available information that is lawfully made available to the general public from federal, state or local governmental records.

Persons Covered

Any data collector that owns or licenses computerized data that includes personal information of a Nevada resident.

Any data collector that maintains computerized data that includes personal information that the data collector does not own.

Encryption/Notification Trigger

The statute only applies to unencrypted data.

Standard for Triggering: The statute is triggered upon discovery or notification of a breach of the security of the system.

Specific Content Requirements

N/A

Timing

A data collector that owns or licenses the information must give notice to affected residents in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system data.

A data collector that maintains the data must give notice to the owner or licensee of the information immediately following discovery of the

breach if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Penalty/Private Right of Action

A private right of action exists for the data collector. A data collector that provides the requisite notice may commence an action for damages against a person who unlawfully obtained or benefited from personal information obtained from records maintained by the data collector.

The Attorney General or a district attorney may bring an action against the person to obtain a temporary or permanent injunction against the violation.

Other Provisions

N/A

BakerHostetler

New Hampshire

N.H. Rev. Stat. Ann. §§ 359-C:19—C:21, 358-A:4 (2006), 332-I:1-I:610; N.H. Rev. Stat. Ann. § 189:65, 189:66

Quick Notes

- New Hampshire has a General Notification Statute for Unauthorized Disclosure of Personal Information, and it has two specific notification statutes: Medical Information Unauthorized Disclosure Notification Statute and Student Data Unauthorized Disclosure Notification Statute.
- "Personal Information" is broader than the general definition because there are two other statutes that specifically protect medical information and student data.
- Notification is not triggered by only access.
- A risk of harm analysis is permitted in determining when notification is triggered.
- A person engaged in trade or commerce shall notify the agency that has primary regulatory authority over such trade or commerce − all other persons shall notify the Attorney General's office.
- An entity regulated by the New Hampshire Insurance Department is required to notify the department of any security breach.
- Notice is not required within an explicit number of days, but it must be made without unreasonable delay.
- A private cause of action is permitted.
- There is an encryption safe harbor.

Personal Information

An individual's first name or first initial with last name with one of the following identifiers:

1. Social Security number.

2. Driver's license or identification card number.

3. Account number, credit or debit card number, security or access code, or password of an individual's financial account.

New Hampshire also has a Medical Information Unauthorized Disclosure Notification Statute and a Student Data Unauthorized Disclosure Notification Statute, each of which provides its own definition of protected information (see full text statute).

Persons Covered

Any person doing business in this state who owns or licenses computerized data that includes personal information, and who discovers a breach of the security of the data; and any person or business who maintains computerized data that includes personal information that the person or business does not own, and who discovers a breach of the security of the data.

Under the Medical Information Unauthorized Disclosure Notification Statute, any person, corporation, facility, or institution either licensed by New Hampshire or otherwise lawfully providing healthcare services, including, but not limited to, a physician, hospital, office, clinic, health center or other healthcare facility.

Under the Student Data Unauthorized Disclosure Notification Stature, the only covered entity is the New Hampshire Department of Education.

Encryption/Notification Trigger

The statute is triggered when a person who owns or licenses computerized data becomes aware of a security breach and determines that misuse of the information has occurred or is reasonably likely to occur.

Both the Medical Information Unauthorized Disclosure Notification Statute and the Student Data Unauthorized Disclosure Notification Statute has its own standard for triggering (see full text statute).

Specific Content Requirements

The following must be included in a notice to affected individuals:

(a) A description of the incident in general terms.

(b) The approximate date of breach.

(c) The type of personal information obtained as a result of the security breach.

(d) The telephonic contact information of the person subject to this section.

The Medical Information Unauthorized Disclosure Notification Statute and Student Data Unauthorized Disclosure Notification Statute each has its own specific content requirements (see full text statute).

Timing

A person who owns or licenses the data must notify the affected individuals as soon as possible after notifying the Attorney General's office. That person is also required to notify a consumer reporting agency without unreasonable delay.

Any person or business who maintains computerized data that includes personal information that the person or business does not own shall notify and cooperate with the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was acquired by an unauthorized person. Cooperation includes sharing with the owner or licensee information relevant to the breach, except that such cooperation shall not be deemed to require the disclosure of confidential or business information or trade secrets.

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

The Medical Information Unauthorized Disclosure Notification Statute requires the covered entity to "promptly notify in writing the individual or individuals whose protected health information was disclosed."

Penalty/Private Right of Action

Persons injured as a result of a violation may bring an action for damages and for such equitable relief as the court deems necessary and proper. A prevailing plaintiff shall be awarded the costs of the suit and reasonable attorneys' fees.

The Attorney General's office shall enforce these provisions by bringing an action in the name of the state to restrain the violation by temporary or permanent injunction, and to obtain up to $10,000 in civil penalties for each violation.

Under the Medical Information Unauthorized Disclosure Notification Statute, an affected individual may bring a civil action.

Other Provisions

Any person engaged in trade or commerce shall notify the regulator that has primary regulatory authority over such trade or commerce; all other persons shall notify the Attorney General's office. Notice to the Attorney General's office must include the anticipated date of the notice to the individuals and the approximate number of individuals in the state who will be notified. The names of the individuals entitled to receive notice do not have to be disclosed.

If a person is required to notify more than 1,000 consumers of a breach of security, the person shall also notify, without unreasonable delay, all consumer reporting agencies of the anticipated date of the notification to the consumers, the approximate number of consumers who will be notified and the content of the notice.

The Student Data Unauthorized Disclosure Notification Statute requires the Department of Education to submit an annual data security breach report to government representatives (see full text statute).

BakerHostetler

New Jersey

N.J. Stat. Ann. § 56:8-163—66 (2005)

Quick Notes

- "Personal Information" is broader than the general definition.
- Notification is triggered by only access.
- A risk of harm analysis is permitted in determining when notification is triggered.
- The Division of State Police in the Law Department of Law and Public Safety must be notified regarding a breach prior to notifying customers.
- Notice is not required within an explicit number of days, but it must be made expediently and without unreasonable delay.
- A private cause of action is not permitted.
- There is an encryption safe harbor.
- The law does not apply to paper records.

Personal Information

An individual's first name or first initial with last name with one of the following identifiers:

1. Social Security number.

2. Driver's license or identification card number.

3. Account number, credit or debit card number, security or access code, or password of an individual's financial account.

4. 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.

Persons Covered

Any entity that conducts business in New Jersey, or any public entity that compiles or maintains computerized records that include personal information.

Any business or public entity that compiles or maintains computerized records that include personal information on behalf of another business or public entity.

Encryption/Notification Trigger

Does not cover encrypted or otherwise unreadable data.

Standard for Triggering: The statute is triggered upon discovery or notification of a breach of security.

Notification is not required if the business or public entity establishes that misuse of the information is not reasonably possible, and a record of this decision must be maintained for five years.

Specific Content Requirements

N/A

Timing

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

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

Penalty/Private Right of Action

It shall be an unlawful practice and a violation of N.J. STAT. ANN. §§ 56:8-1, et seq. to willfully, knowingly or recklessly violate this data breach notification law. Therefore, remedies available under this chapter of the New Jersey Statutes apply to violations of the data breach notification law.

Other Provisions

A breach must be reported to the Division of State Police in the Department of Law and Public Safety prior to notifying customers.

BakerHostetler

New Mexico

2017 H.B. 15, Chap. 36

Quick Notes

- "Personal Information" is broader than the general definition.
- Notification is not triggered by only access.
- A risk of harm analysis is permitted in determining when notification is triggered.
- If more than 1,000 New Mexico residents require notification, notification must be made to the office of the New Mexico Attorney General and the major consumer reporting agencies.
- Notification, to both the affected residents and the New Mexico Attorney General, shall be made in the most expedient time possible, but not later than 45 calendar days following the discovery of the breach.
- A private cause of action is not permitted.
- There is an encryption safe harbor.
- The law does not apply to paper records.

Personal Information (i.e., "Personal Identifying Information")

An individual's first name or first initial with last name with one of the following identifiers:

1. Social Security number.

2. Driver's license or identification card number.

3. Account number, credit or debit card number, security or access code, or password of an individual's financial account.

4. Biometric data, such as an individual's fingerprint, voice print, iris or retina patterns, facial characteristics, or hand geometry.

Persons Covered

A person who owns or licenses elements that include personal identifying information of a New Mexico resident. Any person who is licensed to maintain or possess computerized data containing personal identifying information of a New Mexico resident that the person does not own or license.

Encryption/Notification Trigger

This statute does not apply to encrypted or redacted data unless the confidential process or key used to decrypt the data is compromised such that it compromises the security, confidentiality or integrity of personal identifying information maintained by a person.

Standard for Triggering: The statute is triggered upon discovery of a security breach.

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

Specific Content Requirements

Notification shall contain: (a) the name and contact information of the notifying person, (b) a list of the types of personal identifying information that are reasonably believed to have been the subject of a security breach, if known, (c) 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, (d) a general description of the security breach incident, (e) the toll-free telephone numbers and addresses of the major consumer reporting agencies, (f) advice that directs the recipient to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach, and (g) advice that informs the recipient of the notification of the recipient's rights pursuant to the federal Fair Credit Reporting Act.

Timing

Affected residents shall be notified in the most expedient time possible, but not later than 45 calendar days following discovery of the security breach, subject to the needs of law enforcement and any measures necessary to determine the scope of the security breach and restore the integrity, security and confidentiality of the data system.

Penalty/Private Right of Action

When the Attorney General has a reasonable belief that a violation of the act has occurred, the Attorney General may bring an action on behalf of the individuals and in the name of the state alleging violations of the act.

In any action filed by the Attorney General pursuant to the act, the court may (a) issue an injunction, and (b) award damages for actual costs or losses, including consequential losses.

When a court determines a violation of this section was made knowingly or recklessly, the court may impose a civil penalty of the greater of (a) $25,000 or (b) in the case of failed notification, $10 per instance of failed notification up to a maximum of $150,000.

Other Provisions

If notification is required to be issued to more than 1,000 New Mexico residents as a result of a single security breach, the covered person shall also notify the office of the Attorney General and the major consumer reporting agencies expediently, but not later than 45 calendar days; subject law enforcement and any measures necessary to determine the scope of the security breach; and restore the integrity, security and confidentiality of the data system.

A person required to notify the Attorney General and the major consumer reporting agencies shall disclose the number of New Mexico residents that received notification of the breach and shall provide a copy of the notification sent to the affected residents.

BakerHostetler

New York

N.Y. Gen. Bus. Law § 899-AA (2005)

Quick Notes

- "Personal Information" is not broader than the general definition.
- Notification is not triggered by only access.
- A risk of harm analysis is not permitted in determining when notification is triggered; however, the statute lists factors that may be considered in determining whether unauthorized acquisition of personal information has taken place.
- Notice to the Attorney General, Consumer Protection Board and the state Office of Cyber Security and Critical Infrastructure must be provided regarding a breach via form notice.
- If more than 5,000 New York residents are to be notified at one time, the person or business shall also notify consumer reporting agencies as to the timing, content and distribution of the notices and the approximate number of affected persons.
- Notice is not required within an explicit number of days.
- A private cause of action is not permitted.
- There is an encryption safe harbor unless the encryption key has been acquired by an unauthorized person.
- The law does not apply to paper records.

Personal Information (i.e., "Private Information")

"Private Information" means personal 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 data elements:

1. Social Security number.

2. Driver's license number or non-driver identification card number.

3. Account number, 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.

Persons Covered

Any person or business who conducts business in New York, and who owns or licenses computerized data that includes private information.

Any person or business who maintains computerized data, including private information that such person or business does not own, is covered when there has been a breach of the security of the system.

Encryption/Notification Trigger

When the private information is encrypted and the encryption key has not been acquired, there is no duty to notify.

Standard for Triggering: The statute is triggered upon discovery or notification of an unauthorized acquisition or acquisition without valid authorization of computerized data that compromises the security, confidentiality or integrity of personal information maintained by a business.

A covered entity may consider the following factors in determining whether information has been acquired:

1. Indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information.

2. Indications that the information has been downloaded or copied.

3. Indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

Specific Content Requirements

Notice to residents shall include:

1. Contact information for the covered entity making the notification.

2. A description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so acquired.

Timing

A covered entity must notify affected individuals expediently and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system.

If the covered entity does not own the affected information, the entity must notify the owner or licensee of the information of any breach immediately following discovery, if the private information was, or is reasonably believed to have been, acquired by a person without valid authorization.

Penalty/Private Right of Action

The Attorney General may bring an action in a court having jurisdiction to issue an injunction. The court may award damages for actual costs or losses incurred by a person entitled to notice. Whenever the court determines that a person or business violated this article “knowingly” or “recklessly,” the court may impose a civil penalty of the greater of $5,000 or up to $10,000 per instance of failed notification, provided that the latter amount shall not exceed $150,000.

Any other lawful remedy available can be sought as long as such action is commenced within two years immediately after the date of the act complained of or the date of discovery of such act.

Other Provisions

The person or business must notify the state Attorney General, the Department of State Division of Consumer Protection and the state police as to the timing, content and distribution of the notices and the approximate number of affected persons.

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

BakerHostetler

North Carolina

N.C. Gen. Stat. §§ 75-65 (2005); as amended (2009)

Quick Notes

- "Personal Information" is broader than the general definition.
- Notification is not triggered by only access.
- A risk of harm analysis is permitted in determining when notification is triggered.
- The Consumer Protection Division of the Attorney General's Office must be notified of the nature of the breach, the number of consumers affected, steps taken to investigate the breach, steps taken to prevent a similar breach in the future, and information regarding the timing, distribution and content of the notice via form notice.
- Notice is not required within an explicit number of days, but it must be made without unreasonable delay.
- A private cause of action is permitted only if the individual is injured as a result of the violation. Damages are set at a maximum of up to $5,000 per incident, and provide for treble damages within this range.
- There is an encryption safe harbor.
- The law applies to electronic and paper records.

Personal Information (i.e., "Personal Identifying Information")

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

1. Social Security number or employer taxpayer identification numbers.

2. Driver's license, state identification card, or passport number.

3. Checking and savings account number, credit card number or debit card number, in combination with security or access codes or passwords to an individual's financial account.

4. Digital signature.

5. Biometric data.

6. Fingerprints.

7. Other information that would permit access to a person's financial account or resources.

Personal Information does not include electronic identification numbers, electronic mail names or addresses, internet account numbers, internet identification names, a parent's legal surname prior to marriage, or a password, unless this information would permit access to a person's financial account or resources.

Persons Covered

Any business that owns or licenses personal information in any form (whether computerized, paper or otherwise), or any business that maintains or possesses records or data containing personal information that the business does not own or license.

Encryption/Notification Trigger

Does not cover encrypted information, unless there is unauthorized access to encrypted records along with the confidential process or key.

Standard for Triggering: The statute is triggered upon discovery or notification of a security breach.

Specific Content Requirements

The notice shall be clear and conspicuous and include all of the following: (1) a description of the incident in general terms, (2) a description of the type of personal information that was subject to the unauthorized access and acquisition, (3) a description of the general acts of the business to protect the personal information from further unauthorized access, (4) a telephone number for the business that the person may call for further information and assistance, if one exists, (5) advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports, (6) the toll-free numbers

and addresses of the major consumer reporting agencies, and (7) the toll-free numbers, addresses and website addresses of the FTC and the North Carolina Attorney General's Office, along with a statement that the individual can obtain information from these sources about preventing identity theft.

Timing

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

A covered entity that maintains affected data that it does not own or license must notify the owner or licensee of the information of any security breach immediately following discovery of the breach, consistent with the legitimate needs of law enforcement.

Penalty/Private Right of Action

An individual injured as a result of a violation of this section may institute a civil action. Damages are set at $5,000 per incident, and provide for treble damages within this range. Injunctive relief is also available.

Other Provisions

A breach must be reported to the Consumer Protection Division of the Attorney General's Office. Notification to the Attorney General must include the nature of the breach, the number of consumers affected, steps taken to investigate the breach, steps taken to prevent a similar breach in the future, and information regarding the timing, distribution and content of the notice. Submission of a completed North Carolina Security Breach Reporting Form by mail or fax will satisfy this requirement.

BakerHostetler

North Dakota

N.D. Cent. Code §§ 51-30-01 to -07; 51-15-11; 51-15-07 (2015)

Quick Notes

- "Personal Information" is broader than the general definition.
- Notification is not triggered by only access.
- A risk of harm analysis is not permitted in determining when notification is triggered.
- If the breach involves over 250 individuals, notice must be made to the North Dakota Attorney General by mail or email.
- Notice is not required within an explicit number of days, but it must be made expediently and without unreasonable delay.
- A private cause of action is not permitted.
- There is an encryption safe harbor.
- The law does not apply to paper records.

Personal Information (i.e., "Personal Identifying Information")

An individual's first name or first initial and last name in combination with any of the following data elements, when the name and the data elements are not encrypted:

1. The individual's Social Security number.

2. The operator's license number assigned to an individual by the Department of Transportation.

3. A nondriver color photo identification card number assigned to the individual by the Department of Transportation.

4. The individual's 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 an individual's financial accounts.

5. The individual's date of birth.

6. The maiden name of the individual's mother.

7. Medical information.

8. Health insurance information.

9. An identification number assigned to the individual by the individual's employer in combination with any required security code, access code or password.

10. The individual's digitized or other electronic signature.

Persons Covered

Any person who conducts business in North Dakota and who owns or licenses computerized data that includes personal information.

Any person who maintains computerized data that includes personal information that the person does not own.

Encryption/Notification Trigger

Notification is not required when data has been secured by encryption or by any other method of technology that renders the electronic files, media or databases unreadable or unusable.

Standard for Triggering: The statute is triggered upon discovery or notification of a breach of security.

Specific Content Requirements

Any person who owns or licenses computerized data that includes personal information must disclose any breach of the security system, following discovery or notification of the breach in the security of the

data, to any resident of the state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Timing

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

A person who maintains the data must notify the owner or licensee immediately following discovery of the breach of the security of the system if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Penalty/Private Right of Action

The Attorney General may impose a civil penalty of not more than $5,000 for each violation. The remedies, duties, prohibitions and penalties under this particular law are not exclusive and are in addition to all other causes of action, remedies and penalties.

Other Provisions

Notice to North Dakota Attorney General: Any person who experiences a breach of the security system must disclose to the North Dakota Attorney General by mail or email any breach of the security system that exceeds 250 individuals. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and to restore the integrity of the data system.

BakerHostetler

Ohio

Ohio Rev. Code Ann. §§ 1347.12 (state agencies), 1349.19 (persons and businesses), 1349.191—192 (2007)

Quick Notes

- "Personal Information" is not broader than the general definition.
- Notification is not triggered by only access.
- A risk of harm analysis is permitted in determining when notification is triggered.
- If more than 250 Ohio residents are affected, notice to the Ohio Department of Insurance must be made within 15 days of discovering a "loss of control" of a policyholder's personal information if the covered entity holds a license or certificate of authority from the superintendent of insurance.
- If more than 1,000 residents are affected, consumer reporting agencies must be notified of the timing, distribution and content of the disclosure given to the residents of the state.
- Notice must be provided in the most expedient time possible but not later than 45 days following discovery or notification of a breach.
- A private cause of action is not permitted.
- There is an encryption safe harbor.
- The law does not apply to paper records.

Personal Information (i.e., "Personal Identifying Information")

An individual's first name or first initial with last name with one of the following identifiers:

1. Social Security number.

2. Driver's license or identification card number.

3. Account number, credit or debit card number, in combination with and linked to any required security or access code, or password that would permit access to an individual's financial account.

Persons Covered

Any person, including any business that is conducted in Ohio and that owns, licenses or maintains computerized data that includes personal information.

Any state agency or agency of a political subdivision.

Encryption/Notification Trigger

If the data is encrypted, redacted or altered by any method or technology in such a manner that the data elements are unreadable, it is not considered personal information, and notification is not required.

Standard for Triggering: The statute is triggered upon discovery or notification of a breach of the security of the system.

For a covered entity that is the custodian of the data, the statute is triggered when (1) the entity discovers a breach of the security system, (2) the entity determines that the personal information was, or is reasonably believed to have been, accessed and acquired by an unauthorized person, and (3) the entity determines that the access and acquisition by the unauthorized person caused, or reasonably is believed will cause, a material risk of identity theft or other fraud to a resident of the state.

Specific Content Requirements

N/A

Timing

Affected residents must be notified in the most expedient time possible, but not later than 45 days following discovery or notification of the breach, subject to the legitimate needs of law enforcement and consistent with any measures necessary to (1) determine the scope of the breach, including which residents' personal information was accessed and acquired, and (2) restore the reasonable integrity of the data system.

A state agency, agency of a political subdivision, or person who is the custodian of or stores the data must notify the owner or licensor of the data in an expeditious manner, if the personal information was, or reasonably is believed to have been, accessed and acquired by an unauthorized person, and if the access and acquisition by the unauthorized person causes, or is reasonably believed will cause, a material risk of identity theft or other fraud to a resident of this state.

Penalty/Private Right of Action

The Attorney General may investigate any violations of these sections and bring an action to collect a civil penalty against a person or agency for failing to comply with the statute.

The Attorney General can seek a temporary restraining order, preliminary or permanent injunction, and civil penalties if it appears that a person or agency has failed or is failing to comply with §§ 1347.12 and 1349.19 of the Revised Code.

Upon finding that a person or agency has failed to comply with the statute, the court shall impose a civil penalty as follows:

(a) $1,000 for each day the agency or person has intentionally or recklessly failed to comply with the applicable section, up to 60 days.

(b) $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 the applicable section.

(c) $10,000 for each day AFTER 90 days that the agency or person has intentionally or recklessly failed to comply with the applicable section.

Other Provisions

If more than 1,000 residents are affected, consumer reporting agencies must be notified of the timing, distribution and content of the disclosure given to the residents of the state. An obligation to notify consumer reporting agencies does not permit delaying notification to the affected residents or owner of the data.

BakerHostetler

Oklahoma

Okla. Stat. Tit. 24 § 161 et seq. (2008); Okla. Stat. Tit. 74 § 3113.1 (2006) (public agencies)

Quick Notes

- "Personal Information" is not broader than the general definition.
- Notification is not triggered by only access.
- A risk of harm analysis is permitted in determining when notification is triggered.
- Notice to the Attorney General or State Agency is not required.
- Notice is not required within an explicit number of days, but must be made expediently and without unreasonable delay.
- A private cause of action is not permitted.
- There is an encryption safe harbor.
- The law does not apply to paper records.

Personal Information

An individual's first name or first initial with last name with one of the following identifiers:

1. Social Security number.

2. Driver's license or identification card number.

3. Account number credit or debit card number, in combination with a linked security or access code, or password of an individual's financial account.

Persons Covered

Individuals or entities who own or license computerized data that includes personal information.

Any state agency, board, commission, or other unit or subdivision of state government that owns, licenses or maintains computerized data that includes personal information.

Encryption/Notification Trigger

Notification is not required for encrypted or redacted information, unless the encrypted information is accessed and acquired in an unencrypted form or involves a person with access to the encryption key.

Standard for Triggering: The statute is triggered upon discovery or notification of a breach of the security of the system.

For public agencies, the statute is triggered upon the discovery or notification of any breach of the security of a system when unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Specific Content Requirements

N/A

Timing

Notice to residents shall be made in the most expedient time possible and without unreasonable delay, subject to the needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

A covered entity that maintains affected information that it does not own shall notify the owner or licensee of the information of any breach as soon as practicable following discovery if the personal information was, or was believed to be, accessed and acquired by an unauthorized person.

Any state agency, board, commission, or other unit or subdivision of state government that maintains affected information that it does not own shall notify the owner or licensee of the information of any breach as soon as practicable following discovery if the personal information was, or was believed to be, accessed and acquired by an unauthorized person.

Penalty/Private Right of Action

A violation that results in injury or loss to residents of this state may be enforced by the Attorney General or a district attorney in the same manner as an unlawful practice under the Oklahoma Consumer Protection Act.

The Attorney General or a district attorney shall have exclusive authority to bring an action, and may obtain either an actual 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.

A violation by a state-chartered or state-licensed financial institution shall be enforceable exclusively by the primary state regulator of the financial institution.

Other Provisions

N/A

BakerHostetler

Oregon

Ore. Rev. Stat. §§ 646A.602, 646A.604, 646A.624, as amended (2018)

Quick Notes

- "Personal Information" is broader than the general definition.
- Notification is not triggered by only access.
- A risk of harm analysis is permitted in determining when notification is triggered.
- If more than 250 Oregon residents are affected, the Oregon Attorney General must be notified regarding a breach.
- If more than 1,000 Oregon residents are affected, notice must be made to consumer reporting agencies.
- A person who owns or licenses personal information must provide the Attorney General within a reasonable time at least one copy of any notice the person sends to consumers or to the person's primary or functional regulator.
- Notice must be provided in the most expedient time possible, without unreasonable delay, but not later than 45 days after discovery of the breach.
- A private cause of action is permitted.
- There is an encryption safe harbor.
- The law does not apply to paper records.

Personal Information

A consumer's first name or first initial and last name in combination with any one or more of the following data elements, when the data elements are not rendered unusable through encryption, redaction or other methods, or when the data elements are encrypted and the encryption key has also been acquired:

1. Social Security number, driver's license number or state identification card number issued by the Department of Transportation.

2. Passport number or other United States-issued identification number.

3. 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.

4. Data from measurements of a consumer's physical characteristics, such as an image of a fingerprint, retina or iris, that are used to authenticate the consumer's identity in the course of a financial transaction or other transaction.

5. A consumer's 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.

6. 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.

The data elements above, either in combination or standing alone, are sufficient to be personal information without a first or last name if the information obtained would be sufficient to permit a person to commit identity theft against the consumer whose information was compromised.

Persons Covered

Any person who owns, licenses or otherwise possesses personal information that the person uses in the course of the person's business, vocation, occupation or volunteer activities.

A person (third party) who maintains or otherwise possesses personal information on behalf of another person who owns, licenses or otherwise possesses personal information that the person uses in the course of the person's business, vocation, occupation or volunteer activities shall notify the other person of any breach or suspected breach.

Encryption/Notification Trigger

If the data is encrypted or redacted, notification is not required. If the data is encrypted and the encryption key has also been acquired, notification is required.

Standard for Triggering: The statute is triggered upon discovery or notification of a breach of security from another person who maintains or otherwise possesses personal information on the person's behalf.

For a person who owns the data, notification is not required if, after an appropriate investigation or after consultation with law enforcement, the person determines that no reasonable likelihood of 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.

Specific Content Requirements

Notice shall include at a minimum: (a) a description of the breach of security in general terms, (b) the approximate date of the breach of security, (c) the type of personal information obtained as a result of the breach of security, (d) contact information of the person subject to the statute, (e) contact information for national consumer reporting agencies and (f) advice to the consumer to report suspected identity theft to law enforcement, including the Federal Trade Commission.

Timing

Notice shall be given in the most expeditious time possible and without unreasonable delay, subject to the needs of law enforcement and consistent with any measures necessary to determine sufficient contact information for the consumers, determine the scope of the breach, and restore the reasonable integrity, security and confidentiality of the data.

A third party that maintains data on behalf of another person or entity shall notify the owner or licensor of the information of any breach immediately following discovery of such breach of security if a consumer's personal information was included in the information that was breached.

A person must give notice of a breach of security in the most expeditious manner possible, without unreasonable delay, but not later than 45 days after discovering or receiving notification of the breach of security, subject to the needs of law enforcement.

Penalty/Private Right of Action

Compensation can be ordered by the state upon a finding that enforcement of the rights of consumers by private civil action would be so burdensome or expensive as to be impractical.

In addition to other penalties and enforcement provisions provided by law, any person who violates, or who procures, aids or abets in a violation of, the data breach notification law shall be subject to a penalty of not more than $1,000 per violation, but no more than $500,000 total, which shall be paid to the General Fund of the State Treasury.

Other Provisions

Notice must be given to the Attorney General if more than 250 Oregon residents require notification. Notice must be given to all consumer reporting agencies if more than 1,000 consumers require notification.

A person who owns or licenses personal information shall provide to the Attorney General within a reasonable time at least one copy of any notice the person sends to consumers or to the person's primary or functional regulator.

BakerHostetler

Pennsylvania

73 Pa. Stat. Ann. §§ 2301—2308, 2329 (2006); 201-4, 201-4.1, 201-8 (West 2012)

Quick Notes

- "Personal Information" is not broader than the general definition.
- Notification is not triggered by only access.
- A risk of harm analysis is permitted in determining when notification is triggered.
- Notice to the Attorney General or State Agency is not required.
- If an entity notifies more than 1,000 individuals at one time, the entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution and number of notices.
- Notice is not required within an explicit number of days, but notice must be made without unreasonable delay.
- A private cause of action is not permitted.
- There is an encryption safe harbor.
- The law does not apply to paper records.

Personal Information

An individual's first name or first initial with last name with one of the following identifiers:

1. Social Security number.

2. Driver's license or identification card number.

3. Account number, credit or debit card number, in combination with a linked security or access code, or password of an individual's financial account.

Persons Covered

An entity that maintains, stores or manages computerized data that includes personal information.

A vendor that maintains, stores or manages computerized data on behalf of another entity.

Encryption/Notification Trigger

Notice is required if encrypted information is accessed and acquired in an unencrypted form, if the security breach is linked to a breach of the security of the encryption, or if the security breach involves a person with access to the encryption key.

Standard for Triggering: The statute is triggered when the entity discovers any breach of the security of the system.

Specific Content Requirements

N/A

Timing

An entity shall give notice to affected residents and consumer reporting agencies, if necessary, without unreasonable delay.

A vendor that maintains, stores or manages computerized data on behalf of another entity shall provide notice of any breach of the security system following discovery by the vendor to the entity on whose behalf the vendor maintains, stores or manages the data. The entity shall be responsible for making the determinations and discharging any remaining duties under this act.

Penalty/Private Right of Action

The Attorney General has exclusive authority to bring an action under the Unfair Trade Practices and Consumer Protection Law for a violation of this act.

Other Provisions

When an entity notifies more than 1,000 persons at one time, the entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, of the timing, distribution and number of notices.

BakerHostetler

Puerto Rico

10 L.P.R.A. § 4051; 10 L.P.R.A. § 4052 (2005), as amended (2008)

Quick Notes

- "Personal Information" is broader than the general definition.
- Notification is triggered by only access.
- A risk of harm analysis is not permitted in determining when notification is triggered.
- The Department of Consumer Affairs must be notified regarding a breach as expeditiously as possible (within a nonextendable 10 days after the violation of the system is detected, parties shall inform the Department of Consumer Affairs, which shall make a public announcement of the fact within 24 hours of receiving information).
- Notice is not required within an explicit number of days, but it must be given in the most expedient time possible.
- A private cause of action is permitted.
- There is an encryption safe harbor.
- The law does not apply to paper records.

Personal Information

The first name or first initial and the surname of a person, together with any of the following data so long as it is unencrypted and readable:

1. Social Security number.

2. Driver's license number, voter's identification or other official identification.

3. Bank or financial account numbers of any type with or without passwords or access code that may have been assigned.

4. Names of users and passwords or access codes to public or private information systems.

5. Medical information protected by the HIPAA.

6. Tax information.

7. Work-related evaluations.

Persons Covered

Any entity that is the proprietor or custodian of a data bank for commercial use that includes personal information of citizens who reside in Puerto Rico.

Encryption/Notification Trigger

The statute applies only where information is unencrypted.

Standard for Triggering: The statute is triggered when there has been a violation of the system's security when the data bank whose security has been violated contains all or part of the personal information file, and the same is not protected by a cryptographic code but only by a password.

"Violation of the system's security" means any situation in which it is detected that access has been permitted to unauthorized persons or entities to the data files so that the security, confidentiality or integrity of the information in the data bank has been compromised.

Specific Content Requirements

Notice shall be submitted in a clear and conspicuous manner and should describe the breach in general terms, and the type of sensitive information that was compromised. The notification shall also include a toll-free number and an internet site for people to use in order to obtain information or assistance. Notice can be provided in writing or by authenticated electronic means.

Timing

Clients must be notified as expeditiously as possible, subject to law enforcement and any measures needed to restore the system's

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

Any entity that resells or provides access to digital data banks that at the same time contain personal information files of citizens must notify the proprietor, custodian or holder of said information of any violation of the system's security that has allowed access to those files to unauthorized persons.

Penalty/Private Right of Action

Consumers may bring actions apart from the statute.

The Secretary may impose fines of $500 up to a maximum $5,000 for each violation of the provisions of this act or its regulations. The fines provided in this section do not affect the rights of the consumers to initiate actions or claims for damages before a competent court.

Other Provisions

N/A

BakerHostetler

Rhode Island

R.I. Gen. Laws §§ 11-49.3-2—49.3-6 (2015)

Quick Notes

- "Personal Information" is broader than the general definition.
- Notification is triggered by only access.
- A risk of harm analysis is permitted in determining when notification is triggered.
- If more than 500 Rhode Island residents are affected by a breach, the Rhode Island Attorney General and major credit reporting agencies must be notified as to the timing, content and distribution of the notices and the approximate number of affected Rhode Island residents.
- Notice to the Rhode Island Department of Business Regulation must be made under Insurance Regulation 107 by entities that are licensees of the department, which include insurance companies and producers.
- Notice must be made in the most expedient time possible, but no later than 45 calendar days after confirmation of the breach.
- A private cause of action is not permitted.
- There is an encryption safe harbor.
- The law does not apply to paper records.

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, when the name and the data elements are not encrypted or are in hard copy paper format:

1. Social security number.

2. Driver's license number, Rhode Island identification card number or tribal identification number.

3. Account number, credit card number 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.

4. Medical or health insurance information.

5. Email address with any required security code, access code or password that would permit access to an individual's personal, medical, insurance, or financial account.

Persons Covered

Any municipal agency, state agency, or person who stores, owns, collects, processes, maintains, acquires, uses or licenses data that includes personal information.

Encryption/Notification Trigger

If the information is encrypted, notice is not required.

Standard for Triggering: The statute is triggered following any disclosure of personal information, or any breach of the security of the system, that poses a significant risk of identity theft to any resident of Rhode Island whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person or entity.

Specific Content Requirements

The notification to individuals must include the following information to the extent known: (1) a general description of the incident; (2) the type of information affected; (3) the date or estimated date of the breach; (4) the date that the breach was discovered; (5) a description of any remediation services offered to affected individuals, including toll-free numbers and websites to contact: (i) the credit reporting agencies, (ii) remediation service providers and (iii) the Attorney General; and (6) a description of the consumer's ability to file or obtain a police report, instructions on how a consumer requests a security freeze, and information about fees that may be required to be paid to the consumer reporting agencies.

Timing

Notice must be provided to affected residents in the most expedient time possible and without unreasonable delay, but no later than 45 calendar days after confirmation of the breach, consistent with the legitimate needs of law enforcement.

Notice may be delayed if a law enforcement agency finds delay necessary. Notice shall be provided as soon as practicable after the law enforcement agency determines that notification no longer poses a risk of impeding an investigation.

Penalty/Private Right of Action

Each reckless violation is a civil violation for which a penalty of not more than $100 per occurrence may be adjudged against a defendant. Each knowing and willful violation is a civil violation for which a penalty of not more than $200 per occurrence may be adjudged against a defendant.

Whenever the Attorney General has reason to believe that a violation has occurred, the Attorney General may bring an action against the person or business in violation.

Other Provisions

In the event that more than 500 Rhode Island residents are to be notified, notification shall also be sent to the Attorney General and the major credit reporting agencies as to the timing, content and distribution of the notices, and the approximate number of affected individuals.

Persons or businesses that store personal information shall implement and maintain a risk-based information security program appropriate to the size and scope of the organization, the nature of the information, and the purpose for which the information was collected. The person or business shall not retain the information for a period longer than is reasonably required to provide the services requested.

BakerHostetler

South Carolina

S.C. Code § 1-11-490 (2008); S.C. Code § 39-1-90 (2009)

Quick Notes

- "Personal Information" is broader than the general definition.
- Notification is not triggered by only access.
- A risk of harm analysis is permitted in determining when notification is triggered.
- If 1,000 or more persons are affected, the Consumer Protection Division of the Department of Consumer Affairs must be notified regarding a breach.
- Notice is not required within an explicit number of days, but it must be made expediently and without unreasonable delay.
- A private cause of action is permitted.
- There is an encryption safe harbor.
- The law does not apply to paper records.

Personal Information

An individual's first name or first initial with last name with one of the following identifiers:

1. Social Security number.

2. Driver's license or identification card number.

3. Account number, credit or debit card number, in combination with a linked security or access code, or password of an individual's financial account.

4. Other numbers or information that may be used to access a person's financial accounts, or numbers or information issued by a governmental or regulatory entity that will uniquely identify an individual.

Persons Covered

Any person (business or individual) or agency who does business in South Carolina and owns, maintains or licenses computerized data that includes personal identifying information about a resident of South Carolina.

Encryption/Notification Trigger

If data is rendered unusable through encryption, redaction or other methods, notice is not required.

Standard for Triggering: The statute is triggered upon discovery or notification of a breach of the security of the system.

Specific Content Requirements

N/A

Timing

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

An entity that maintains affected information that it does not own or license must notify the owner or licensee of the information of a breach immediately following discovery if the personal identifying information was, or is reasonably believed to have been, acquired by an unauthorized person.

Penalty/Private Right of Action

A resident who is injured by a violation of the statute, in addition to and cumulative of all other rights and remedies available at law, may institute a civil action to recover damages in case of a willful and

knowing violation; institute a civil action to recover only actual damages resulting from a violation in case of a negligent violation; seek an injunction to enforce compliance; and recover attorneys' fees and court costs, if successful.

A person or agency that knowingly and willfully violates the data breach notification laws is subject to an administrative fine of up to $1,000 for each resident whose information was accessible by reason of the breach, the amount to be decided by the Department of Consumer Affairs.

Other Provisions

A breach must be reported to the Consumer Protection Division of the Department of Consumer Affairs if 1,000 or more persons were affected.

An entity that maintains its own notification procedures as part of an information security policy for the treatment of personal identifying information and is otherwise consistent with the timing requirements of this section, is considered to be in compliance with the notification requirements of this section if the person notifies subject persons in accordance with required policies in the event of a breach of security of the system.

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 is considered to be in compliance with the data breach notification laws.

BakerHostetler

South Dakota

Senate Bill 62 (2018)

Quick Notes

- "Personal Information" is broader than the general definition.
- Notification is not triggered by only access.
- A risk of harm analysis is permitted in determining when notification is triggered.
- If more than 250 South Dakota residents are affected by the breach, an information holder must notify the South Dakota Attorney General.
- Notice is required no later than 60 days from the discovery or notification of the breach. If notification was delayed by law enforcement, notification must be made 30 days after the law enforcement agency determines that notification will not compromise the criminal investigation.
- A private cause of action is not permitted.
- There is an encryption safe harbor.
- The law does not apply to paper records.

Personal Information

An individual's first name or first initial with last name with one of the following identifiers:

1. Social Security number.

2. Driver's license or identification card number.

3. Account number, credit or debit card number, in combination with a linked security or access code, or password of an individual's financial account.

4. Health information as defined by the Health Insurance Portability and Accountability Act.

5. 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.

6. The username or email address in combination with a password, security question, and answer or other information that permits access to an online account.

Persons Covered

Any information holder, meaning any person or business who conducts business in South Dakota and who owns or licenses computerized personal or protected information of residents of this state.

Encryption/Notification Trigger

Standard for Triggering: The statute is triggered following the discovery by or notification to an information holder of a breach of system security.

Notice is not required, however, if, following an appropriate investigation and notice to the Attorney General, the information holder reasonably determines that the breach will not likely result in harm to the affected person. The information holder shall document the determination under this section in writing and maintain the document for not less than three years.

Specific Content Requirements

N/A

Timing

Notice shall be provided not later than 60 days from the discovery or notification of the breach of the system security, unless a longer period of time is required due to the legitimate needs of law enforcement.

If notification is delayed due to a determination by law enforcement that notification will impede a criminal investigation, then notification shall be made not later than 30 days after the law enforcement agency determines that notification will not compromise the criminal investigation.

Penalty/Private Right of Action

The Attorney General may prosecute each failure to make a required disclosure as a deceptive act or practice. In addition, the Attorney General may bring action to recover on behalf of the state a civil penalty of not more than $10,000 per day per violation. The Attorney General may recover attorneys' fees and costs associated with any action brought under this section.

Other Provisions

An information holder shall disclose to the Attorney General, by mail or email, any breach of system security that exceeds 250 residents.

An information holder required to provide notice to affected persons shall also notify, without unreasonable delay, the nationwide credit reporting agencies.

BakerHostetler

Tennessee

Tenn. Code Ann. §§ 47-18-2105 to -2107 (2005); as amended (2016, 2017)

Quick Notes

- "Personal Information" is not broader than the general definition.
- Notification is not triggered by only access.
- A risk of harm analysis is permitted in determining when notification is triggered.
- Notice to the Attorney General or State Agency is not required.
- Notice is required immediately, but no later than 45 days from the discovery of the breach.
- A violation under the data breach notification statute may also be a violation of the Tennessee Consumer Protection Act, which could give rise to a private cause of action.
- There is an encryption safe harbor.
- The law does not apply to paper records.

Personal Information

An individual's first name or first initial with last name with one of the following identifiers:

1. Social Security number.

2. Driver's license or identification card number.

3. Account number, credit or debit card number, in combination with a linked security or access code, or password of an individual's financial account.

Persons Covered

Any person or business who conducts business in Tennessee, or any agency of the state of Tennessee or any of its political subdivisions that owns, licenses or maintains computerized data that includes personal information.

Encryption/Notification Trigger

Standard for Triggering: The statute is triggered upon discovery or notification of a breach of the security of the system.

"Breach of the security of the system" means the acquisition of information by an unauthorized person that materially compromises the security, confidentiality or integrity of personal information maintained by the information holder, where the information that is acquired consists of either:

(i) Unencrypted computerized data.

(ii) Encrypted computerized data and the encryption key.

Specific Content Requirements

N/A

Timing

Notification must be provided immediately, but no later than 45 days from the discovery or the notification of the breach.

A covered entity that maintains affected data, including personal information that it does not own or license, shall notify the owner or licensee of the information of any breach immediately, but no later than 45 days from discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification shall be made no later than 45 days after the law enforcement agency determines that it will not compromise its investigation.

Penalty/Private Right of Action

Any customer of the information holder who is a person or business entity may institute a civil action to recover damages and enjoin the person or business entity from further action in violation. However, a customer cannot be an agency of the state or any political subdivision of the state.

In addition, a violation can subject the violator to a civil penalty of $10,000; $5,000 per day that a person's identity has been assumed; or 10 times the amount obtained or attempted to be obtained through the identity theft, whichever is greater. The Attorney General can also seek injunctions and get attorneys' fees. A violation under this statute may also be a violation of the Tennessee Consumer Protection Act.

Other Provisions

N/A

BakerHostetler

Texas

Texas Bus. & Com. Code § 521.002 and 521.053 (2007); as amended (2012)

Quick Notes

- "Personal Information" is broader than the general definition.
- Notification is not triggered by only access.
- A risk of harm analysis is not permitted in determining when notification is triggered.
- Notice to Texas Department of Insurance pursuant to Commissioner's Bulletin # B-0022-16A, a domestic insurer or HMO should contact its assigned financial analyst at the Texas Department of Insurance if the insurer or HMO experiences or discovers an unauthorized acquisition, release, or use of personal information or sensitive company information.
- Notice is not required within an explicit number of days, but it should be provided "as quickly as possible."
- A violation under the data breach notification statute may also be a violation of the Texas Deceptive Trade Practices Act, which could give rise to a private cause of action.
- There is an encryption safe harbor.
- The law does not apply to paper records.

Personal Information

An individual's first name or first initial with last name with one of the following identifiers:

1. Social Security number.

2. Driver's license or identification card number.

3. Account number, credit or debit card number, in combination with a linked security or access code, or password of an individual's financial account.

4. 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 payment for the provision of healthcare to the individual.

Persons Covered

A person who conducts business in this state and owns, licenses or maintains computerized data that includes sensitive personal information.

Encryption/Notification Trigger

Sensitive personal information only includes data items that are not encrypted unless the encryption key is also breached.

Standard for Triggering: The statute is triggered upon discovery or the receipt of notification of a breach of system security.

Specific Content Requirements

N/A

Timing

Disclosure should be made as quickly as possible or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system. However, disclosure may be delayed at the request of a law enforcement agency that determines that the notification will impede a criminal investigation.

Any person who maintains computerized data that includes sensitive personal information not owned by the person shall notify the owner or license holder of the information of any breach of system security immediately after discovering the breach, if the sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Penalty/Private Right of Action

The Attorney General may bring a civil suit for damages or an injunction. A person who violates the statute is liable to the state for a civil penalty of at least $2,000 but not more than $50,000 for each violation.

A person who fails to comply with notification requirements is liable to the state for a civil penalty of not more than $100 for each individual to whom notification is due for each consecutive day the person fails to take reasonable action to notify, with a maximum penalty of $250,000 for a single breach.

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

A violation of this statute is also a deceptive trade practice under the Texas Deceptive Trade Practices Act, which permits a private action.

Other Provisions

If an entity must notify over 10,000 individuals of a breach, the entity must notify each consumer reporting agency of the timing, distribution and content of the notices without unreasonable delay.

Businesses must implement and maintain reasonable procedures, including appropriate corrective action, to protect from unlawful use or disclosure of sensitive personal information, such as shredding, erasing or other similar means of modifying sensitive personal information, to make it unreadable or indecipherable. This section does not apply to a financial institution.

BakerHostetler

U.S. Virgin Islands

14 V.I.C. § 2208, et seq. (2005)

Quick Notes

- "Personal Information" is not broader than the general definition.
- Notification is not triggered by only access.
- A risk of harm analysis is not permitted in determining when notification is triggered.
- Notice to the Attorney General or State Agency is not required.
- Notice is not required within an explicit number of days, but it must be given in the most expedient time possible and without unreasonable delay.
- A private cause of action is permitted.
- There is an encryption safe harbor.
- The law does not apply to paper records.

Personal Information

An individual's first name or first initial with last name with one of the following identifiers:

1. Social Security number.

2. Driver's license or identification card number.

3. Account number, credit or debit card number, in combination with a linked security or access code, or password of an individual's financial account.

Persons Covered

Any agency that owns or licenses computerized data that includes personal information; any agency that maintains (but does not own) computerized data that includes personal information; and any person or business who conducts business in the Virgin Islands and who owns or licenses computerized data that includes personal information; any person or business who maintains computerized data that includes personal information the person or business does not own.

Encryption/Notification Trigger

Statute applies only where personal information was unencrypted.

Standard for Triggering: Any agency, person or business that owns or licenses computerized data with personal information shall disclose any breach following discovery or notification of the breach in security of the data to any resident of the Virgin Islands whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

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

Specific Content Requirements

N/A

Timing

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

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

Penalty/Private Right of Action

Any customer injured by a violation may commence a civil action to recover damages. Any business that violates, proposes to violate or has violated this title may be enjoined. The rights and remedies available are cumulative to each other and to any other rights and remedies available under law.

Other Provisions

N/A

BakerHostetler

Utah

Utah Code Ann. §§ 13-44-101—301 (2006); as amended (2009)

Quick Notes

- "Personal Information" is not broader than the general definition.
- Notification is not triggered by only access.
- A risk of harm analysis is permitted in determining when notification is triggered.
- Notice to the Attorney General or State Agency is not required.
- Notice is not required within an explicit number of days, but it should be provided in the most expedient time possible and without unreasonable delay.
- A private cause of action is not permitted.
- There is an encryption safe harbor.
- The law does not apply to paper records.

Personal Information

An individual's first name or first initial with last name with one of the following identifiers:

1. Social Security number.

2. Driver's license or identification card number.

3. Account number, credit or debit card number, in combination with a linked security or access code, or password of an individual's financial account.

Persons Covered

Any person who conducts business in the state and owns, maintains or licenses computerized information that contains personal information.

Encryption/Notification Trigger

If the personal information is encrypted or protected by another method that renders the data unreadable or unusable, it is not protected, and notice is not required.

Standard for Triggering: The statute is triggered when a person covered by the statute becomes aware of a breach of system security, at which time the covered person must conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused for identity theft or fraud purposes.

Specific Content Requirements

N/A

Timing

A person required to provide notification shall provide the notification in the most expedient time possible without unreasonable delay, considering legitimate investigative needs of law enforcement, after determining the scope of the breach of system security, and after restoring the reasonable integrity of the system.

A person who maintains computerized data that includes personal information that the person does not own or license shall notify and cooperate with the owner or licensee of the information of any breach, immediately following the person's discovery of the breach, if misuse of the personal information occurs or is reasonably likely to occur.

Cooperation includes sharing information relevant to the breach with the owner or licensee of the information.

Penalty/Private Right of Action

The statute does not create a private right of action, but likewise does not affect any private right of action that may exist under other law, including contract or tort.

A person who violates this subchapter is subject to a civil fine of (a) no greater than $2,500 for a violation or series of violations concerning a specific consumer, and (b) no greater than $100,000 in the aggregate for related violations concerning more than one consumer.

The Attorney General may also seek injunctive relief.

Other Provisions

Any person who conducts business in the state and maintains personal information shall implement and maintain reasonable procedures to prevent unlawful use or disclosure of personal information collected or maintained in the regular course of business, and shall destroy, or arrange for the destruction of, records containing personal information that are not to be retained by the person. The destruction of records shall be by shredding, erasing or otherwise modifying the personal information to make the information indecipherable.

BakerHostetler

Vermont

Vt. Stat. Ann. Tit. 9, §§ 2430, 2435 (2006); as amended (2008); as amended (2012)

Quick Notes

- "Personal Information" is broader than the general definition.
- Notification is not triggered by only access.
- A risk of harm analysis is permitted in determining when notification is triggered.
- Once notice is made to consumers, the Attorney General must be notified of the number of Vermont consumers affected and provided a copy of the notice. If the covered entity provides notice to more than 1,000 consumers at one time, all consumer reporting agencies must be notified as to the timing, distribution and content of the notices being sent to the affected customers.
- Notice shall be made in the most expedient time possible and without unreasonable delay, but not later than 45 days after discovery.
- A private cause of action is not permitted.
- There is an encryption safe harbor.
- The law does not apply to paper records.

Personal Information

An individual's first name or first initial with last name in combination with any one or more of the following digital data elements, when either the name or the data elements are not encrypted, redacted or otherwise protected:

1. Social Security number.

2. Driver's license or identification card number.

3. Account number, credit or debit card number, in combination with a linked security or access code, or password of an individual's financial account.

4. Account passwords or personal identification number or other access codes for a financial account.

Persons Covered

Any data collector that owns or licenses computerized personally identifiable information that includes personal information concerning a consumer, or that maintains or possesses computerized data containing personally identifiable information of a consumer that the data collector does not own or license, or any data collector that acts or conducts business in Vermont that maintains or possesses records or data containing personally identifiable information that the data collector does not own or license.

Encryption/Notification Trigger

Data is not considered personally identifiable information if both the individual's name and the combined data element are encrypted, redacted or protected by another method that renders them unreadable or unusable.

Standard for Triggering: The statute is triggered upon discovery or notification of a security breach.

Notice of a security breach is not required if the data collector establishes that misuse of personal information is not reasonably possible. Notice of the determination shall be provided to the Vermont Attorney General's Office or to the Department of Financial Regulation.

If the data collector later gathers facts to indicate that the misuse of personal information is reasonably possible, then notice is required.

Specific Content Requirements

Notice shall be clear and conspicuous, and shall include a description of the following:

(a) The incident in general terms.

(b) The type of personally identifiable information that was subject to the security breach.

(c) The general acts of the data collector to protect the personally identifiable information from further unauthorized access or acquisition.

(d) A telephone number, toll-free if available, that the consumer may call for further information and assistance.

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

(f) The approximate date of the security breach.

Timing

Notice of the security breach to a consumer shall be made in the most expedient way possible and without unreasonable delay, but not later than 45 days after discovery.

Within 14 business days of the discovery of the incident, the Attorney General must be provided the date of the security breach, date of discovery and a preliminary description of the breach.

Penalty/Private Right of Action

The Attorney General and state's attorney shall have sole and full authority to investigate potential violations and to enforce, prosecute, obtain and impose remedies for any violation.

Other Provisions

Once notice is made to consumers, the Attorney General must be notified of the number of Vermont consumers affected and provided a copy of the notice. A second copy of the consumer notification letter, with personally identifiable information that was subject to the breach redacted, can also be provided to the Attorney General, which will be used for any public disclosure of the breach. For Vermont-regulated financial institutions, notice should be made instead to the Department of Financial Regulation.

In the event a data collector provides notice to more than 1,000 consumers at one time pursuant to this section, the data collector shall notify, without unreasonable delay, all consumer reporting agencies. In notice to a consumer reporting agency, the data collector must include the timing, distribution and content of the notices being sent to the affected consumers.

BakerHostetler

Virginia

Va. Code Ann. § 18.2-186.6 (2008) Va. Code Ann. § 32.1—127.1:05 (2011)

Quick Notes

- Virginia has a Personal Information Breach Notification Statute and a Medical Information Breach Notification Statute.
- "Personal Information" is broader than the general definition because it includes "Medical Information."
- Notification is not triggered by only access.
- A risk of harm analysis is permitted in determining when notification is triggered.
- The Attorney General must be notified following discovery of a breach of personal information. If more than 1,000 persons were notified at one time, notice must also be made to all consumer reporting agencies of the timing, distribution and content of the notice sent to affected residents.
- The Attorney General and the commissioner of health must be notified following discovery of a breach of medical information.
- Notice shall be made in the most expedient time possible and without unreasonable delay, but not later than 45 days after discovery.
- A private cause of action is permitted. Nothing in the data breach notification statute will preclude recovery of economic damages.
- There is an encryption safe harbor.
- The law does not apply to paper records.

Personal Information

An individual's first name or first initial with last name with one of the following identifiers:

1. Social Security number.

2. Driver's license or identification card number.

3. Account number, credit or debit card number, in combination with a linked security or access code, or password of an individual's financial account.

The Medical Information Breach Notification Statute has its own definition of medical information (see full-text statute).

Persons Covered

An individual or entity who owns or licenses computerized data that includes personal information, and an individual or entity who maintains computerized data that includes personal information that the individual or entity does not own or license, are covered under the Personal Information Breach Notification Statute.

An entity that owns or licenses computerized data that includes medical information, and an entity that maintains computerized data that includes medical information that the entity does not own or license, are covered under the Medical Information Breach Notification Statute.

The statute does not apply to (i) a person or entity who is a "covered entity" or "business associate" under HIPAA (42 USC § 1320d et seq.) or (ii) a person or entity who is a non-HIPAA-covered entity subject to the Health Breach Notification Rule promulgated by the Federal Trade Commission pursuant to 42 USC § 17937 et seq.

Encryption/Notification Trigger

Neither statute applies to encrypted, redacted or altered information that is rendered unusable unless the encrypted data is accessed and acquired in unencrypted form or in combination with the encryption key.

Standard for Triggering: The Personal Information Notification Statute is triggered when a person covered by the statute discovers or is notified of a breach of the security of the system.

Notwithstanding the above, the statute is triggered for any employer or payroll service provider that owns or licenses computerized data relating to income tax withholding upon the discovery or notification of unauthorized access and acquisition of unencrypted and unredacted computerized data containing taxpayer personal information.

The Medical Information Breach Notification Statute is triggered upon discovery or notification of a breach of the security of the system.

Specific Content Requirements

Under the Personal Information Breach Notification Statute, notice must include a description of (1) the incident in general terms; (2) the type of personal information that was subject to the unauthorized access and acquisition; (3) the general acts of the entity to protect the personal information from further unauthorized access; (4) a telephone number that the person may call for further information and assistance, if one exists; and (5) advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports.

Under the Medical Information Breach Notification Statute, notice must include a description of (1) the incident in general terms; (2) the type of medical information that was subject to the unauthorized access and acquisition; (3) the general acts of the entity to protect the medical information from further unauthorized access; and (4) a telephone number that the person may call for further information and assistance, if one exists.

Timing

Notice under both statutes must be given without unreasonable delay, subject to law enforcement and any measures necessary to restore the integrity of the data system.

Under the Personal Information Breach Notification Statute, a covered entity that does not own or license the affected information it maintains shall notify the owner or licensee of the information of any breach of the security of the system without unreasonable delay following discovery of the breach of the security of the system.

Under the Medical Information Breach Notification Statute, a covered entity that does not own or license the affected information it maintains shall notify the owner or licensee of the information of any breach of the security of the system without unreasonable delay following discovery of the breach of the security of the system.

Penalty/Private Right of Action

Under the Personal Information Breach Notification Statute, the Attorney General may bring an action to address violations by imposing a civil penalty not to exceed $150,000 per breach of the security of the system. Nothing shall limit an individual from recovering direct economic damages from a violation of this law.

A violation by a state-chartered or licensed financial institution shall be enforceable exclusively by the financial institution’s primary state regulator. A violation of this section by an individual or entity regulated by the State Corporation Commission’s Bureau of Insurance shall be enforced exclusively by the State Corporation Commission.

Other Provisions

Under the Personal Information Breach Notification Statute, the Office of the Attorney General must be notified following discovery of a breach of personal information.

In the event an individual or entity provides notice to more than 1,000 persons at one time, the individual or entity must notify, without unreasonable delay, both the Office of the Attorney General and all consumer reporting agencies of the timing, distribution and content of the notice sent to affected residents.

For incidents involving a taxpayer identification number in combination with the income tax withheld for that taxpayer, the entity must notify the Office of the Attorney General without delay and provide the name and federal employer identification number of the employer.

Under the Medical Information Breach Notification Statute, the Office of the Attorney General and the commissioner of health must be notified following discovery of a breach of medical information. The entity must notify both the subject of the medical information and any affected resident of the commonwealth, if those are not the same person.

In the event an entity provides notice to more than 1,000 persons at one time, the entity must notify, without unreasonable delay, the Office of the Attorney General and the commissioner of health of the timing, distribution and content of the notice sent to affected individuals.

BakerHostetler

Washington

Wash. Rev. Code Ann. §§ 19.255.010, 19.255.020 (2005) Wash. Rev. Code Ann. §§ 42.56.590 (2005); as amended (2015)

Quick Notes

- "Personal Information" is not broader than the general definition.
- Notification is not triggered by only access.
- A risk of harm analysis is permitted in determining when notification is triggered.
- The Attorney General must be notified no later than 45 days following discovery of a breach of personal information that required notice to more than 500 individuals.
- All licensees must provide notice to the Office of the Insurance Commissioner within two business days of such licensee determining that notification regarding a security breach of personal health or private information under RCW 19.255.010 and 45 C.F.R. 164 is required to be made to consumers or customers.
- Notice shall be made in the most expedient time possible and without unreasonable delay, but not later than 45 calendar days after discovery.
- A private cause of action is permitted.
- There is an encryption safe harbor.
- The law applies to electronic and paper records.

Personal Information

An individual's first name or first initial with last name with one of the following identifiers:

1. Social Security number.

2. Driver's license or identification card number.

3. Account number, credit or debit card number, in combination with a linked security or access code, or password of an individual's financial account.

Persons Covered

Any person, business or agency who conducts business in Washington and who owns or licenses any data (computerized or hard copy) that includes personal information of residents of Washington, and any person, business or agency who maintains computerized data that includes personal information the person, business or agency does not own.

Encryption/Notification Trigger

If both an individual's first name or first initial and last name and accompanying data element are encrypted, notice is not required.

Standard for Triggering: The statute is triggered upon discovery or notification of a breach in the security of the system.

A person, business or agency shall not be required to disclose a technical breach of the security system that does not seem reasonably likely to subject customers to risk of harm.

Data that is "secured" (encrypted or otherwise protected) is not subject to the data breach notification requirements unless the encryption key was accessed by an unauthorized person.

Specific Content Requirements

Any person or business that is required to issue notification must meet all of the following requirements:

a. The notification must be written in plain language.

b. The notification must include, at a minimum, the following information:

i. The name and contact information of the reporting person or business.

ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

iii. The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed personal information.

Timing

Notice must be given to residents and to the Washington Attorney General in the most expedient time possible and without unreasonable delay, no more than 45 calendar days after the breach was discovered, subject to the needs of law enforcement and any measures necessary to determine the scope of the breach.

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

Penalty/Private Right of Action

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

Any person, business or agency that violates, proposes to violate or has violated this statute may be enjoined. The rights and remedies available are cumulative to each other and to any other rights and remedies available under the law.

Other Provisions

Notice to the Washington Attorney General: Any person or business that is required to issue notification under RCW 19.255.010 and 42.56.590 to more than 500 Washington residents as a result of a single breach must, no more than 45 days after the breach is discovered, electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Washington Attorney General.

Notice to Office of the Insurance Commissioner: As adopted under notice filed as WSR 13-07-053, all licensees must notify the insurance commissioner within two business days of such licensee determining that notification regarding a security breach of personal health or private information under RCW 19.255.010 and 45 C.F.R. 164 is required to be made to consumers or customers.

The Washington Attorney General may bring an action in the name of the state, or on behalf of persons residing in the state, to enforce the law.

BakerHostetler

West Virginia

W. Va. Code Ann. §§ 46A-2A-101-104 (2008)

Quick Notes

- "Personal Information" is not broader than the general definition.
- Notification is not triggered by only access.
- A risk of harm analysis is permitted in determining when notification is triggered.
- Notice to the Attorney General or State Agency is not required. However, if more than 1,000 individuals must be notified at one time, then all consumer reporting agencies must be notified.
- Notice is not required within an explicit number of days, but it should be provided in the most expedient time possible and without unreasonable delay.
- A private cause of action is not permitted.
- There is an encryption safe harbor.
- The law does not apply to paper records.

Personal Information

An individual's first name or first initial with last name with one of the following identifiers:

1. Social Security number.

2. Driver's license or identification card number.

3. Account number, credit or debit card number, in combination with a linked security or access code, or password of an individual's financial account.

Persons Covered

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

Encryption/Notification Trigger

If encrypted or redacted information is accessed and acquired and the person does not have access to the encryption key, notice is not required.

Standard for Triggering: The statute is triggered upon discovery or notification of a breach of the security of the system.

Specific Content Requirements

The notice shall include:

(1) 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.

(2) 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:

(A) What types of information the entity maintained about that individual or about individuals in general.

(B) Whether or not the entity maintained information about that individual.

(3) The 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.

When notifying consumer reporting agencies, an individual or entity must include information on the timing, distribution and content of the notices being sent to the affected residents.

Timing

An individual or entity who owns or licenses data must notify a resident of the security breach without unreasonable delay, unless:

(1) A law enforcement agency determines and advises the individual or entity that the notice will impede a criminal or civil investigation or homeland or national security.

(2) The individual or entity needs to take any measures necessary to determine the scope of the breach.

(3) The individual or entity needs time to restore the reasonable integrity of the system.

A covered entity that does not own or license the affected information that it maintains shall give notice to the owner or licensee of the information of any breach of the security of the system as soon as practicable following discovery, if the personal information was, or the entity reasonably believes the information was, accessed and acquired by an unauthorized person.

Penalty/Private Right of Action

Failure to comply constitutes an unfair or deceptive act of practice, which may be enforced by the Attorney General. The Attorney General shall have exclusive authority to bring action. No civil penalty may be assessed in an action unless the court finds that the defendant has engaged in a course of repeated and willful violations.

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. A violation by a licensed financial institution shall be enforceable exclusively by the financial institution’s primary functional regulator.

Other Provisions

If an entity is required to notify more than 1,000 persons of a breach, the entity shall also notify, without unreasonable delay, all consumer reporting agencies of the timing, distribution and content of the notices. The entity must not provide to the consumer reporting agency the names or other personal identifying information of breach notice recipients.

This subsection shall not apply to an entity that is subject to Title V of the Gramm Leach Bliley Act, 15 U.S.C. 6801, et seq.

BakerHostetler

Wisconsin

Wis. Stat. Ann. § 134.98 (2006); as amended (2008)

Quick Notes

- "Personal Information" is broader than the general definition.
- Notification is not triggered by only access.
- A risk of harm analysis is permitted in determining when notification is triggered.
- Notice to the Attorney General or State Agency is not required. However, if more than 1,000 individuals must be notified at one time, then all consumer reporting agencies must be notified.
- Wisconsin licensed insurers, gift annuities, warranty plans, motor clubs and employee benefit plan administrators are requested to notify the office of any unauthorized access to personal information of Wisconsin residents as soon as practicable, but not later than 10 days after it becomes aware of such unauthorized access.
- Notice shall be provided within a reasonable time, not to exceed 45 days after the entity learns of the acquisition of personal information.
- A private cause of action is not permitted.
- There is an encryption safe harbor.
- The law applies to electronic and paper records.

Personal Information

An individual's first name or first initial with last name with one of the following identifiers:

1. Social Security number.

2. Driver's license or identification card number.

3. Account number, credit or debit card number, in combination with a linked security or access code, or password of an individual's financial account.

4. DNA profile.

5. The individual's unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation.

Persons Covered

An entity whose principal place of business is located in Wisconsin or an entity that maintains or licenses personal information in Wisconsin, and knows personal information in the entity's possession has been acquired by a person whom the entity has not authorized to acquire the personal information; or an entity whose principal place of business is not located in Wisconsin, but who knows that personal information pertaining to a resident of Wisconsin has been acquired by a person whom the entity has not authorized to acquire the information.

Encryption/Notification Trigger

If one of the data elements linked to an individual's name is encrypted, redacted or altered in a manner that renders the element unreadable, no notice is required.

Standard for Triggering: The statute is triggered when a person or entity knows that a person whom the entity has not authorized to acquire personal information has acquired the personal information.

If a covered entity knows that personal information in the entity's possession has been acquired by an unauthorized person, the entity shall make reasonable efforts to notify each subject of the personal information. The notice shall indicate that the entity knows of the unauthorized acquisition of personal information pertaining to the subject of the personal information.

If an entity whose principal place of business is not located in this state knows that personal information pertaining to a resident of this state has been acquired by an unauthorized person, the entity shall make reasonable efforts to notify each resident of this state who is the subject of the personal information. The notice shall indicate that the entity knows of the unauthorized acquisition of personal information pertaining to the resident of this state who is the subject of the personal information.

If a person, other than an individual, that stores personal information pertaining to a resident of this state, but does not own or license the personal information, knows that the personal information has been acquired by an unauthorized person, and the person storing the personal information has not entered into a contract with the person who owns or licenses the personal information, the person storing the personal information shall notify the person that owns or licenses the personal information of the acquisition as soon as practicable.

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

Specific Content Requirements

Notice to the subject of acquired personal information shall indicate that the entity knows of the unauthorized acquisition of personal information pertaining to the subject of the personal information.

Upon written request by a person who has received notice, the entity that provided the notice shall identify the personal information that was acquired.

Timing

Notice shall be provided within a reasonable time, not to exceed 45 days after the entity learns of the acquisition of personal information. A determination as to reasonableness shall include consideration of the number of notices that an entity must provide and the methods of communication available to the entity.

Penalty/Private Right of Action

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

Other Provisions

If a person or entity must notify 1,000 or more individuals, the entity must notify all consumer reporting agencies of the timing, distribution and content of the notices sent to the individuals.

The statute does not apply to an entity subject to privacy and security requirements of 15 U.S.C. § 6801-6827, or to a person who has a contractual obligation to such entity, if the entity or person has in effect a policy concerning breaches of information security. Likewise, the statute does not apply to an entity described in 45 CFR § 164.104(a), if the entity complies with the requirements of 45 CFR part 164.

BakerHostetler

Wyoming

Wyo. Stat. Ann. §§ 40-12-501, 40-12-502 (2015)

Quick Notes

- "Personal Information" is broader than the general definition.
- Notification is not triggered by only access.
- A risk of harm analysis is permitted in determining when notification is triggered.
- Notice to the Attorney General or State Agency is not required.
- Notice is not required within an explicit number of days, but it must be given as soon as possible, in the most expedient time possible, and without unreasonable delay.
- A private cause of action is not permitted.
- There is an encryption safe harbor.
- The law does not apply to paper records.

Personal Information

An individual's first name or first initial with last name with one of the following identifiers:

1. Social Security number.

2. Driver's license or identification card number.

3. Account number, credit or debit card number, in combination with a linked security or access code, or password of an individual's financial account.

4. Tribal identification card.

5. Federal or state government-issued identification card.

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

7. Birth or marriage certificate.

8. Medical information, meaning a person's medical history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional.

9. 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.

10. Unique biometric data, meaning data generated from measurements or analysis of human body characteristics for authentication purposes.

11. Individual taxpayer identification number.

Persons Covered

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

Encryption/Notification Trigger

If both an individual's first name or first initial and last name and combined data element are redacted, notice is not required.

Standard for Triggering: The statute is triggered when an individual or entity becomes aware of a breach of the security of the system and, after a prompt, reasonable and good faith investigation, the individual or commercial entity determines that the misuse of personal identifying

information about the residents has occurred or is reasonably likely to occur.

Specific Content Requirements

Notice shall include a toll-free number that the individual may use to contact the person collecting the data, or his or her agent; and from which the individual may learn the toll-free contact telephone numbers and addresses of the major credit reporting agencies.

Notice must be clear and conspicuous and must meet six other requirements (see full text statute).

Timing

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

Any person who maintains computerized data that includes personal identifying information on behalf of another business entity shall disclose to the business entity for which the information is maintained any breach as soon as practicable following the determination that personal identifying information was, or is reasonably believed to have been, acquired by an unauthorized person.

Penalty/Private Right of Action

The Attorney General may bring an action in law or equity to address any violation and for other relief that may be appropriate to ensure proper compliance, to recover damages or both.

Other Provisions

N/A