Arent Fox

SEPTEMBER 2019

Arent Fox LLP Survey of Data Breach Notification Statutes

James Westerlind

Survey Overview

This Survey focuses on the data breach notification statutes of the states and territories within the US, and should be a useful tool and guide for data security planning and response purposes.

Smart In Your World

arentfox.com

September 2019

We are pleased to share with you the third version of Arent Fox LLP's Survey of Data Breach Notification statutes within the United States and its territories. This Survey includes amendments and new statutes that have been enacted since August of last year, and provides answers to the key initial questions that a company should have with respect to state data breach notification statutes if it learns that the personal identifiable information that it maintains for its customers or employees, or on behalf of other companies that it does business with, has been, or likely has been, breached or used in an unauthorized manner. Namely:

(1) Which statutes in a particular jurisdiction apply?

(2) Who must comply with the notification requirements?

(3) What data is covered by the statutes?

(4) What constitutes a data breach?

(5) Who must be notified pursuant to the statute?

(6) When must notice be sent?

(7) In what form or manner must notice be sent?

(8) What must the notice say?

(9) Are there any exemptions?

(10) Who may enforce the requirements and what penalties may be imposed for violations?

(11) Are there any data security requirements imposed?

(12) Are there any industry-specific requirements?

This updated Survey focuses on the data breach notification statutes of the states and territories within the U.S., and should be a useful tool and guide for data security planning and response purposes. If your company experiences a data security incident, one of the first things that you must consider is the potential scope of the incident and whose personal information may be implicated. If you have customers who reside in multiple jurisdictions and whose personal information may have been breached, you will have to analyze the data breach notification rules of each of those jurisdictions and comply with each. While most of the statutes are similar, many have particular nuances that differ, and a failure to comply may result in additional problems and liability for your company. This Survey is intended to make that task easier for you.

In addition to state and territory specific statutes, you will also have to consider the applicability of various federal laws and private industry requirements (*e.g.*, HIPAA and the HITECH Act; the Gramm-Leach-Bliley Act; and Payment Card Industry requirements) and, if your company does business outside the U.S., the laws of other countries (*e.g.*, the EU General Data Protection Regulation, which became enforceable on May 25, 2018, and Canada's Personal Information Protection and Electronic Documents Act, which becomes effective November 1, 2018). While this Survey does not address these additional laws, feel free to give us a call if you have any questions about them.

We hope that you find this survey useful.

James Westerlind

TABLE OF CONTENTS

Page

TABLE OF CONTENTS (cont'd.)

Page

INTRODUCTION

By James Westerlind[1]

Every state and territory[2] in the U.S. has a data breach notification statute.

Most of the data breach notification statutes apply to any person, business or government agency that acquires, owns or licenses computerized data that includes personal identifiable information of individuals who reside within that jurisdiction. Personal identifiable information is typically defined to include the resident's name (*e.g.*, first name or initial and last name) in combination with any one or more of the following data elements that relate to the resident, when the data elements are not encrypted, redacted, or secured by any other method rendering the name or the element unreadable or unusable: (1) social security number; (2) driver's license number or state identification number; and (3) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial account. In addition, as the type of data that is collected and stored grows in complexity and breadth, some states have now included biometric data (*e.g.*, iris, retina, or fingerprint scans) in the definition of personal identifiable information. *See, e.g.*, Iowa Code § 715C(11)(5); Colo. Rev. Code § 716(1)(g)(I)(A); and, most recently, Arkansas (HB 1943).

A data breach is typically defined as the unauthorized acquisition, or reasonable belief of unauthorized acquisition, of personal information that compromises the security, confidentiality, or integrity of that data maintained by the entity. Most statutes exclude from the definition of data breach data that: (1) was encrypted or substantially redacted; (2) is already publicly available through lawful means; or (3) was improperly acquired in good faith by an employee or agent of the entity for the legitimate purposes and is not otherwise used or subject to further unauthorized disclosure. Some jurisdictions define "encryption," and others do not. Those jurisdictions that define the word usually do so in general terms, such as the "transformation of data through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key, or securing information by another method that renders the data elements unreadable or unusable." Mich. Comp. Laws § 445.63(g). But other jurisdictions, such as Massachusetts and Rhode Island, have greater specificity in their definitions of the term. *See, e.g.*, Mass. Gen. Laws 93H § 1(a) and R.I. Gen. Laws § 11-49.3-3(a) (each requiring the use of use of a 128-bit or higher algorithmic process).

The statutes generally require notification to be provided to those individuals residing within the jurisdiction whose personal identifiable information has been, or may have been, compromised. Some jurisdictions allow companies to perform a good faith, reasonable, and prompt investigation to determine if misuse of customer information has occurred, or is reasonably likely to occur. If the company determines in these jurisdictions that misuse has not occurred, or is unlikely, it will not be required to send data breach notifications to customers in that jurisdiction. *See, e.g.,* Md. Code, Commercial Law § 14-3504(b).

---

[1] James Westerlind is Counsel in Arent Fox's litigation, insurance, cybersecurity & data protection, and automotive practice groups. Thanks and acknowledgment to Andrew Dykens, Jeff Leung, Lee Pepper, Alexandra Coppola, Stephen Blake, and Ashley Baxter for their hard work and assistance in the revision of this Survey.

[2] The term "territory" or "territories" refers only to Unincorporated Organized Territories. This Survey does not apply to other U.S. Territories.

In addition, some jurisdictions require notice to be provided to the Attorney General of the state, other state agencies (including, in many instances, law enforcement), or credit reporting agencies (or all of these institutions), depending on the number of residents within the state to whom notice must be sent. Notice typically must be sent in the most expeditious time possible and without unreasonable delay, and may only be delayed in some jurisdictions if law enforcement determines that notice should be delayed for purposes of its investigation of the matter, or for any measures necessary to determine the scope of the breach, prevent further disclosures, and restore the reasonable integrity of the company's system. Some jurisdictions have short notification deadlines. Vermont, for instance, requires a data collector to provide a preliminary description of the breach to the Attorney General or Department of Financial Regulation within 14 business days of discovering the breach. *See* Vt. Stat. Ann. tit. 9 § 2435(b)(3)(B)(i).

Generally, notice must be provided in one of the following ways: (1) in writing; (2) electronically, if the entity's primary method of communication with the individual is by electronic means;[3] (3) by telephone;[4] or (4) by substitute notice. Substitute notice is usually permitted only if the entity demonstrates that the cost of providing notice through the other permissible manners would exceed a certain dollar threshold (which amount varies by jurisdiction), or that the affected class of subject individuals to be notified exceeds a certain number (which number also varies by jurisdiction), or the entity does not have sufficient contact information. If substitute notice is permitted, it typically must be sent in all of the following manners: (a) email, if the entity has an email address for the resident; (b) conspicuously posting the disclosure on the website of the entity, if the entity maintains a website; and (c) providing a notice to major statewide media.

Many jurisdictions do not specify what the notice must say to affected residents or regulators. Those jurisdictions that do have specificity in this regard generally require the notice to provide: (1) to the extent possible, a description of the categories of information that were, or are reasonably believed to have been, acquired by an unauthorized person, including which of the elements of personal information were, or are reasonably believed to have been, acquired; (2) contact information for the entity making the notification, including address, telephone number, and toll-free telephone number if one is maintained; (3) the toll-free telephone numbers and addresses for the major consumer reporting agencies; and (4) the toll-free telephone numbers, addresses, and website addresses for state and federal regulatory agencies. *See, e.g.*, Md. Code, Commercial Law § 14-3504(g). In addition, in those jurisdictions that specify what notice to the regulators must say, such notice must typically provide: (1) a synopsis of the events surrounding the breach at the time notice is provided; (2) the number of individuals in the 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 entity to affected individuals; (4) a copy of the notice to be provided to state residents; and (5) the name, address, telephone number, and email address of the employee or agent of the entity from whom additional information may be obtained about the breach. *See, e.g.*, Fla. Stat. § 501.171(3)(b). In addition, some states require covered entities to offer credit monitoring services free of charge for a

[3] Some jurisdictions also allow electronic notice if making the disclosure by electronic means is consistent with the provisions regarding electronic records and signatures required for notices legally required to be in writing under 15 U.S.C. § 7001 (Electronic Signatures in Global and National Commerce Act). *See, e.g.*, Alaska Stat. § 45.48.030.
[4] Missouri requires that direct contact be made with the affected individual if notice is provided by telephone. *See* Mo. Rev. Stat. § 407.1500(2)(6)(c).

specified period of time (typically, one year) to consumers whose personal identifying information has been exposed in a data breach. *See* Conn. Gen. Stat. § 36a-701b(b)(2)(B); Del. Code 6, § 12B-102(e).

In some jurisdictions, violations of breach notification laws can only be enforced by the Attorney General, while in certain other jurisdictions residents can sue in their own right. And some jurisdictions impose specific statutory penalties for violations of their breach notification statutes.

In addition, some jurisdictions have more recently enacted certain data security requirements. Furthermore, some states have imposed industry-specific breach notification requirements.

The following are notable amendments and statutory enactments which occurred over the past year:

- Arkansas: Arkansas amended its data breach statute to include biometric information of an individual in its definition of personal information; a requirement for a company that has experienced a data breach to give notice to the Attorney General in the event that personal information of more than 1,000 users has been, or is believed to have been, breached; and a requirement that companies maintain written determinations of a breach of the security of their systems for a period of five years.

- Connecticut: Effective October 1, 2018, Connecticut expanded its definition of personal information in its data breach notification statute to include credit and debit cards as a separate category, without the necessity of access to the associated financial account.

- Maryland: Effective October 1, 2018, penalty caps will be increased to $10,000 for each violation, and $25,000 for each subsequent act repeating the same violation. In addition, effective October 1, 2019, Maryland amended its data breach notification statute to: (1) add the "Insurance – Breach of Security of a Computer System – Notification Requirement," which requires certain carriers to notify the Maryland Insurance Commissioner within 45 days that a certain breach of the security of a system has occurred; and (2) add procedures for when the breached business is not the owner or licensee of the computerized data.

- Massachusetts: Effective April 10, 2019, certain language must be included in a breach notification letter to affected consumers, the State Attorney General, and the office of consumer affairs and business regulation. The requirements include whether the organization implemented a written information security program.

- Michigan: Effective January 20, 2020, entities regulated by the Michigan Insurance Code are exempt from the state's data breach notification statute, but such companies will be regulated by new statutes within the Michigan Insurance Code.

- Mississippi: Effective July 1, 2019, Mississippi's "Insurance Data Security Law" will regulate those persons/entities licensed under Mississippi insurance laws.

- New Hampshire: Effective August 11, 2018, New Hampshire added robust protections for personal information of students or teachers required to be maintained by the state's Department of Education, which must establish, and update annually, minimum standards for maintaining the privacy and security of student and employee data for local education agencies.

- New Jersey: Effective September 1, 2019, the definition of "personal information" was expanded to include "user name, email address, or any other account holder identifying information, in combination with any password or security question and answer that would permit access to an online account." In addition, the company breached may provide notification in electronic or other form that directs the customer to promptly change any password to protect the online account with the business, but the business that furnishes an email account shall not provide notification to the email account that is subject to a security breach.

- Ohio: Effective March 20, 2019, new standards have been enacted for data security and for the investigation of and notification to the Superintendent of Insurance of a cybersecurity event. The new statutory provisions are based upon the National Association of Insurance Commissioners' Insurance Data Security Model Law (also referred to as "MDL-668"). Ohio has now become the second state to adopt a version of MDL-668, joining South Carolina.

- Texas: Effective September 1, 2019, Texas' data breach notification will create a privacy council to provide privacy advice to the legislature to support possible future comprehensive privacy legislation. Effective January 1, 2020, Texas' data breach notification statute will require a person who is required to disclose or provide notification of a breach of system of security to also notify the attorney general of the breach (including specified information) not later than 60 days after the date on when the person determines that the breach occurred if the breach involves at least 250 residents of the state.

Back to TOC

ALABAMA

STATUTE: Ala. Code § **8-38-1** ***et seq.***,[5] Ala. Code § 8-19-11.

WHO MUST COMPLY?

Under § 8-38-2(2), a "covered entity," which is defined as a person, sole proprietorship, partnership, government entity, corporation, nonprofit, trust, estate, cooperative association, or other business entity that acquires or uses sensitive personally identifying information, must comply.

Under § 3, each covered entity and third-party agent shall implement and maintain reasonable security measures to protect sensitive personally identifying information against a breach of security.

WHAT DATA IS COVERED?

Under § 8-38-2(6)(a), "Sensitive Personally Identifying Information" is defined as an Alabama resident's first name or first initial and last name in combination with one or more of the following with respect to the same Alabama resident:

(1) A non-truncated Social Security number or tax identification number.

(2) A non-truncated driver's license number, state-issued identification card number, passport number, military identification number, or other unique identification number issued on a government document used to verify the identity of a specific individual.

(3) A financial account number, including a bank account number, credit card number, or debit card number, in combination with any security code, access code, password, expiration date, or PIN, that is necessary to access the financial account or to conduct a transaction that will credit or debit the financial account.

(4) Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

(5) An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual.

(6) A user name or email address, in combination with a password or security question and answer that would permit access to an online account affiliated with the covered entity that is reasonably likely to contain or is used to obtain sensitive personally identifying information.

[5] Publicly available at: http://arc-sos.state.al.us/PAC/SOSACPDF.001/A0012674.PDF (last visited June 12, 2019).

Under § 8-38-2(6)(b), "Sensitive Personally Identifying Information" does not include either of the following:

(1) Information about an individual which has been lawfully made public by a federal, state, or local government record or a widely distributed media.

(2) Information that is truncated, encrypted, secured, or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable, including encryption of the data, document, or device containing the sensitive personally identifying information, unless the covered entity knows or has reason to know that the encryption key or security credential that could render the personally identifying information readable or useable has been breached together with the information.

WHAT CONSTITUTES A DATA BREACH?

Under § 8-38-2(1), a "breach of security" or "breach" is defined as the unauthorized acquisition of data in electronic form containing sensitive personally identifying information. Additionally, acquisition occurring over a period of time committed by the same entity constitutes one breach.

A "breach" does not include any of the following:

(1) Good faith acquisition of sensitive personally identifying information by an employee or agent of a covered entity, unless the information is used for a purpose unrelated to the business or subject to further unauthorized use.

(2) The release of a public record not otherwise subject to confidentiality or nondisclosure requirements.

(3) Any lawful investigative, protective, or intelligence activity of a law enforcement or intelligence agency of the state, or a political subdivision of the state.

WHOM MUST BE NOTIFIED?

Under § 8-38-5(a), a covered entity that determines, as a result of a breach of security, sensitive personally identifying 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 person to whom the information relates, shall give notice of the breach to each person to whom the information relates.

Under § 8-38-6(a), if the number of individuals a covered entity is required to notify exceeds 1,000, the entity shall provide written notice of the breach to the Attorney General.

Under § 8-38-7, if a covered entity is required to provide notice to more than 1,000 individuals at a single time, the entity shall also notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis

WHEN MUST NOTICE BE SENT?

Under § 8-38-5(b), notice must be sent as expeditiously as possible and without unreasonable delay, taking into account the time necessary to allow the covered entity to conduct an investigation. Additionally, notice must be made within 45 days of discovering that a breach has occurred and is reasonably likely to cause substantial harm to the individuals to whom the information relates.

Under § 8-38-6(a), if the Attorney General must be notified, the entity shall provide written notice to the Attorney General as expeditiously as possible and without unreasonable delay. In such a scenario, notice must be made within 45 days of discovering that a breach has occurred or is reasonably likely to cause substantial harm to the individuals to whom the information relates.

Additionally, under § 8-38-6(c), a covered entity may provide the Attorney General with supplemental or updated information regarding a breach at any time.

Under § 8-38-7, if a covered entity is required to provide notice to all consumer reporting agencies, notice must be provided without unreasonable delay.

IN WHAT FORM AND MANNER MUST NOTICE BE SENT?

Under § 8-38-5(d), notice to an affected individual shall be in writing, sent to the mailing address of the individual in the records of the covered entity, or by email notice sent to the email address of the individual in the records of the covered entity.

Under § 8-38-5(e)(1), a covered entity required to provide notice to any individual under this section may provide substitute notice in lieu of direct notice, if direct notice is not feasible due to any of the following:

(1) Excessive cost, including either of the following:

(a) Excessive cost to the covered entity relative to the resources of the covered entity.

(b) The cost to the covered entity exceeds five hundred thousand dollars ($500,000).

(2) Lack of sufficient contact information for the individual required to be notified.

(3) The affected individuals exceed 100,000 persons.

Under § 8-38-5(e)(2)(a), substitute notice shall include both of the following:

(1) A conspicuous notice on the Internet website of the covered entity, if the covered entity maintains a website, for a period of 30 days.

(2) Notice in print and in broadcast media, including major media in urban and rural areas where the affected individuals reside.

Finally, under § 8-38-5(e)(2)(b), an alternative form of substitute notice may be used with the approval of the Attorney General.

Under § 8-38-6(a), if a covered entity is required to give notice to the Attorney General, it must be in writing.

WHAT MUST THE NOTICE SAY?

Under § 8-38-5(d), notice shall include, at a minimum, all of the following:

(1) The date, estimated date, or estimated date range of the breach.

(2) A description of the sensitive personally identifying information that was acquired by an unauthorized person as part of the breach.

(3) A general description of the actions taken by a covered entity to restore the security and confidentiality of the personal information involved in the breach.

(4) A general 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.

Under § 8-38-6(b), written notice to the Attorney General shall include all of the following:

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

(2) The approximate number of individuals in the state who were 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 on how to use the services.

(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 about the breach.

Under § 8-38-7, if a covered entity is required to give notice to all consumer reporting agencies, they must notify them of the time, distribution, and content of the notices that were provided to individuals under § 8-38-5.

ARE THERE ANY EXEMPTIONS?

Under § 8-38-5(c), if a federal or state law enforcement agency determines that notice to individuals would interfere with a criminal investigation or national security, notice shall be delayed upon the receipt of written request of the law enforcement agency for a period that the

law enforcement agency determines is necessary. Additionally, the law enforcement agency, by a subsequent written request, may revoke the delay or extend the period set forth in the original request if further delay is necessary. Under § 8-38-6(a), this same exception exists for providing notice to the Attorney General.

Under § 8-38-5(f), if a covered entity determines that notice is not required, the entity shall document the determination in writing and maintain records concerning the determination for no less than five years.

Under § 8-38-9(b)(6), government entities are exempt from civil penalties; however, the Attorney General may bring an action against any state, county, or municipal official or employee, in his or her official capacity, who is subject to this chapter for any of the following:

(1) To compel the performance of his or her duties under this Act.

(2) To compel the performance of his or her ministerial acts under this Act.

(3) To enjoin him or her from acting in bad faith, fraudulently, beyond his or her authority, or under mistaken interpretation of the law.

Under § 8-38-11, an entity subject to or regulated by federal laws, rules, regulations, procedures, or guidance on data breach notification established or enforced by the federal government is exempt from this act so long as the entity does all of the following:

(1) Maintains procedures pursuant to those laws, rules, regulations, procedures, or guidance.

(2) Provides notice to affected individuals pursuant to those laws, rules, regulations, procedures, or guidance.

(3) Timely provides a copy of the notice to the Attorney General when the number of individuals the entity notified exceeds 1,000.

Under § 8-38-12, an entity subject to or regulated by state laws, rules, regulations, procedures, or guidance on data breach notification that are established or enforced by state government, and are at least as thorough as the notice requirements provided by this act, is exempt from this act so long as the entity does all of the following:

(1) Maintains procedures pursuant to those laws, rules, regulations, procedures, or guidance.

(2) Provides notice to affected individuals pursuant to the notice requirements of those laws, rules, regulations, procedures, or guidance.

(3) Timely provides a copy of the notice to the Attorney General when the number of individuals the entity notified exceeds 1,000.

Back to TOC

WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

Under § 8-38-9(a), the Attorney General has exclusive authority to bring an action for civil penalties under this act.

Under § 8-38-9(a)(2), any covered entity or third-party agent who willfully or with reckless disregard fails to provide notice to individuals or the Attorney General is subject to the penalty provisions set out in Ala. Code § 8-19-11. Civil penalties shall not exceed $500,000 per breach.

Further, a covered entity that violates the notification provisions of this chapter shall be liable for a civil penalty of up to $5,000 per day for each consecutive day the entity fails to take reasonable action to comply with the notice provisions.

ARE THERE ANY DATA SECURITY REQUIREMENTS IMPOSED?

Under § 8-38-3(a), each covered entity and third-party agent shall implement and maintain reasonable security measures to protect sensitive personally identifying information against a breach of security.

Under § 8-38-3(b), "reasonable security measures" means security measures practicable for the covered entity to implement and maintain, including consideration of all of the following:

(1) Designation of an employee or employees to coordinate the covered entity's security measures to protect against a breach of security. An owner or manager may designate himself or herself.

(2) Identification of internal and external risks of a breach of security.

(3) Adoption of appropriate information safeguards to address identified risks of a breach of security and assess the effectiveness of such safeguards.

(4) Retention of service providers, if any, that are contractually required to maintain appropriate safeguards for sensitive personally identifying information.

(5) Evaluation and adjustment of security measures to account for changes in circumstances affecting the security of sensitive personally identifying information.

(6) Keeping the management of the covered entity, including its board of directors, if any, appropriately informed of the overall status of its security measures.

Under § 8-38-3(c), an assessment of a covered entity's security shall be based upon the entity's security measures as a whole and shall place an emphasis on data security failures that are multiple or systemic, including consideration of all the following:

(1) The size of the covered entity.

(2) The amount of sensitive personally identifying information and the type of activities for which the sensitive personally identifying information is accessed, acquired, maintained, stored, utilized, or communicated by, or on behalf of, the covered entity.

(3) The covered entity's cost to implement and maintain the security measures to protect against a breach of security relative to its resources.

ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

None.

ALASKA

STATUTE: Alaska Stat. § 45.48.010 ***et seq.***[6]

WHO MUST COMPLY?

Under § 45.48.010(a), a "covered person" who owns or licenses personal information in any form must comply. "Covered person" is defined under § 45.48.090(2) as a (A) person doing business; (B) governmental agency; or (C) person with more than 10 employees.

WHAT DATA IS COVERED?

Under § 45.48.010(a), "personal information" is covered. "Personal information" is defined under § 45.48.090(7) as:

(1) an individual's name. "Individual's name" means a combination of an individual's:

  (a) first name or first initial; and

  (b) last name; and

(2) one or more of the following information elements:

  (a) the individual's social security number;

  (b) the individual's driver's license number or state identification card number;

  (c) with certain exceptions, the individual's account number, credit card number, or debit card number;

  (d) if an account can only be accessed with a personal code, the account number and the personal code; in this sub-subparagraph, "personal code" means a security code, an access code, a personal identification number, or a password;

  (e) passwords, personal identification numbers, or other access codes for financial accounts.

WHAT CONSTITUTES A DATA BREACH?

Under § 45.48.090(1), "breach of the security" means unauthorized acquisition, or reasonable belief of unauthorized acquisition, of personal information that compromises the security, confidentiality, or integrity of the personal information maintained by the information collector.

[6] Publicly available at: *Laws Of Alaska 2008,* http://www.legis.state.ak.us/PDF/25/Bills/HB0065Z.PDF (last visited June 12, 2019).

Under § 45.48.050, the good faith acquisition of personal information by an employee or agent of an information collector for a legitimate purpose of the information collector is not a breach of the security of the information system if the employee or agent does not use the personal information for a purpose unrelated to the legitimate purpose of the information collector and does not make further unauthorized disclosures of the personal information.

WHO MUST BE NOTIFIED?

Under § 45.48.010 (a), if a breach occurs, the covered entity must notify each state resident whose personal information was subject to the breach. Additionally, under § 45.48.040, if notification of more than 1,000 state residents is required, the information collector shall also notify without unreasonable delay all consumer credit reporting agencies that compile and maintain files on consumers on a nationwide basis and provide the agencies with the timing, distribution, and content of the notices to state residents.

WHEN MUST NOTICE BE SENT?

Under § 45.48.010(b), an information collector, defined in § 45.48.090(4) as any covered person who owns or licenses personal information in any form if the personal information includes personal information on a state resident, shall make the disclosure in the most expeditious time possible and without unreasonable delay, except as necessary for law enforcement purposes or to determine the scope of the breach and restore the reasonable integrity of the information system.

IN WHAT FORM AND MANNER MUST NOTICE BE SENT?

Under § 45.48.030, notice may be provided in one of the following manners:

(1) by a written document sent to the most recent address the information collector has for the state resident;

(2) by electronic means if the information collector's primary method of communication with the state resident is by electronic means or if making the disclosure by the electronic means is consistent with the provisions regarding electronic records and signatures required for notices legally required to be in writing under 15 U.S.C. 7001 (Electronic Signatures in Global and National Commerce Act); or

(3) if the information collector demonstrates that the cost of providing notice would exceed $150,000, that the affected class of state residents to be notified exceeds 300,000, or that the information collector does not have sufficient contact information to provide notice, by:

(a) electronic mail if the information collector has an electronic mail address for the state resident;

(b) conspicuously posting the disclosure on the Internet website of the information collector if the information collector maintains an Internet website; and

(c) providing a notice to major statewide media.

WHAT MUST THE NOTICE SAY?

No specific requirement. The notice must simply disclose the breach to each state resident whose personal information was subject to the breach.

ARE THERE ANY EXEMPTIONS?

Under § 45.48.010(c), disclosure is not required if, after an appropriate investigation and after written notification to the attorney general of this state, the covered person determines that there is not a reasonable likelihood that harm to the consumers whose personal information has been acquired has resulted or will result from the breach.

Under § 45.48.020, an information collector may delay disclosing the breach if an appropriate law enforcement agency determines that disclosing the breach will interfere with a criminal investigation. However, after the law enforcement agency informs the information collector in writing that disclosure of the breach will no longer interfere with the investigation, the information collector shall disclose the breach to the state resident in the most expeditious time possible and without unreasonable delay.

Under § 45.48.040(c), an information collector required to notify more than 1,000 state residents of a breach does not have to notify all consumer reporting credit agencies that compile and maintain files on consumers on a nationwide basis if the information collector is subject to the Gramm-Leach-Bliley Financial Modernization Act.

WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

Under § 45.48.080,

(1) If an information collector who is a governmental agency violates §§ 45.48.010--45.48.090 with regard to the personal information of a state resident, the information collector (1) is liable to the state for a civil penalty of up to $500 for each state resident who was not notified under §§ 45.48.010--45.48.090, but the total civil penalty may not exceed $50,000; and (2) may be enjoined from further violations.

(2) If an information collector who is not a governmental agency violates §§ 45.48.010--45.48.090 with regard to the personal information of a state resident, the violation is an unfair or deceptive act or practice under §§ 45.50.471--45.50.561. However, (1) the information collector is not subject to the 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 § 45.48.010--45.48.090, except that the total civil penalty may not exceed $50,000; and (2) damages that may be awarded against the information collector under (A) § 45.50.531 are limited to actual economic damages that do not exceed $500; and (B) § 45.50.537 are limited to actual economic damages.

(3) The Department of Administration may enforce (a) of this section against a governmental agency. The procedure for review of an order or action of the department under this subsection is the same as the procedure provided by § 44.62 (Administrative Procedure Act), except that the office of administrative hearings (§ 44.64.010) shall conduct the hearings in contested cases and the decision may be appealed under § 44.64.030(c).

ARE THERE ANY DATA SECURITY REQUIREMENTS IMPOSED?

None.

ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

None.

Back to TOC

ARIZONA

STATUTE: Ariz. Rev. Stat. §§ **18-551, 18-552**[7]

WHO MUST COMPLY?

Under § 18-552(A), a person that conducts business in Arizona and that owns, maintains or licenses unencrypted and unredacted computerized data that includes personal information must comply.

WHAT DATA IS COVERED?

Under § 18-551(7), "personal Information" is covered, and means:

(1) An individual's first name or first initial and last name in combination with one or more Specified Data Elements.

(2) An individual's user name or e-mail address, in combination with a password or security question and answer, that allows access to an online account.

"Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media.

Under §18-551(11), "Specified Data Element" means any of the following:

(1) an individual's social security number.

(2) the number on an individual's driver license issued pursuant to section 28-3166 or nonoperating identification license issued pursuant to section 28-3165.

(3) a private key that is unique to an individual and that is used to authenticate or sign an electronic record.

(4) an individual's financial account number or credit or debit card number in combination with any required security code, access code or password that would allow access to the individual's financial account.

(5) an individual's health insurance identification number.

(6) information about an individual's medical or mental health treatment or diagnosis by a health care professional.

(7) an individual's passport number.

[7] Publicly available at: *Title 18 – Information Technology*, https://www.azleg.gov/arsDetail/?title=18.

(8) an individual's taxpayer identification number or an identity protection personal identification number issued by the United States Internal Revenue Service.

(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.

WHAT CONSTITUTES A DATA BREACH?

Under § 18-551(1)(a), a "breach" or "security breach" means an unauthorized acquisition of and unauthorized access that materially compromises the security or confidentiality of unencrypted and unredacted computerized personal information maintained as part of a database of personal information regarding multiple individuals.

"Security breach" does not include a good faith acquisition of personal information by a person's employee or agent for the purposes of the person if the personal information is not used for a purpose unrelated to the person and is not subject to further unauthorized disclosure.

WHO MUST BE NOTIFIED?

Under § 18-552(B), if an investigation results in a determination that there has been a breach in a security system, the individuals affected shall be notified.

If the breach requires notification of more than one thousand individuals, notify both:

(1) the three largest nationwide consumer reporting agencies; and

(2) the attorney general, in writing, in a form prescribed by rule or order of the attorney general or by providing the attorney general with a copy of the notification provided to affected individuals.

WHEN MUST NOTICE BE SENT?

The notice shall be made within forty-five days after the determination that a breach has occurred subject to delay if a law enforcement agency advises the person that the notifications will impede a criminal investigation. § 18-552(B)(1), (D).

IN WHAT FORM AND MANNER MUST NOTICE BE SENT?

Under § 18-552(F), notice must be provided by one of the following methods:

(1) written notice;

(2) an e-mail notice if the person has e-mail 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 the person demonstrates that the cost of providing notice pursuant to paragraphs (1)-(3) of this subsection would exceed $50,000, that the affected class of subject individuals to be notified exceeds 100,000 individuals, or that the person does not have sufficient contact information.

Substitute notice shall consist of: (a) a written letter to the attorney general that demonstrates the facts necessary for substitute notice; and (b) conspicuous posting of the notice for at least forty-five days on the web site of the person if the person maintains one.

WHAT MUST THE NOTICE SAY?

Under § 18-552(E), the notice must include at least the following:

(1) The approximate date of the breach;

(2) A brief description of the personal information included in the breach;

(3) The 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 or any federal agency that assists consumers with identity theft matters.

ARE THERE ANY EXEMPTIONS?

Under § 18-552(H), a person that maintains their own notification procedure as part of an information security policy for the treatment of personal information and that is otherwise consistent with the requirements of this article, including the 45-day notification period, is deemed to be in compliance with the notification requirements if the person notifies subject individuals in accordance with the person's policies if a security system breach occurs.

Under § 18-552(I), a person that complies with the notification requirements or security system breach procedures pursuant to the rules, regulations, procedures, guidance or guidelines established by the person's primary or functional federal regulator is deemed to be in compliance with the notice requirements of subsection B, paragraph 1 of this section.

Under § 18-552(J), a person is not required to make the notification required by subsection B of this section if the person, an independent third-party forensic auditor or a law enforcement agency determines after a reasonable investigation that a security system breach has not resulted in or is not reasonably likely to result in substantial economic loss to affected individuals.

Under § 18-552(N), this statute does not apply to either of the following:

(1) a person that is subject to title V of the Gramm-Leach-Bliley act (P.L. 106-102; 113 Stat. 1338; 15 U.S.C. §§ 6801 - 6809); or

(2) a covered entity or business associates as defined under regulations implementing the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), 45 Code of Federal Regulations section 160.103 (2013) or a charitable fund-raising foundation or nonprofit corporation whose primary purpose is to support a specified covered entity, if the charitable fund-raising foundation or nonprofit corporation complies with any applicable provision of the health insurance portability and accountability act of 1996 and its implementing regulations.

WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

Under § 18-552(L), this section may only be enforced by the Attorney General. A knowing and willful violation of the law constitutes a violation of the Arizona Consumer Fraud Act, § 44-1521 *et seq*. The Attorney General may recover restitution for a knowing and willful violation of this section and may impose a civil penalty not to exceed the lesser of $10,000 per affected individual or the total amount of economic loss sustained by affected individuals, but the maximum civil penalty from a breach or series of related breaches may not exceed $500,000.

ARE THERE ANY DATA SECURITY REQUIREMENTS IMPOSED?

None.

ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

None.

Back to TOC

ARKANSAS

STATUTE: Ark. Code § **4-110-101** ***et seq.***[8] Amended by **Arkansas Laws Act 1030 (H.B. 1943)** (effective August 9, 2019).[9]

WHO MUST COMPLY?

Under § 4-110-105(a)(1), any person or business that acquires, owns or licenses computerized data that includes personal information must comply.

Under § 4-110-105(b)(1), a 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 that there has been a breach of the security of the system immediately following discovery if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. If a breach of this nature affects more than 1,000 individuals, the person or business is required to make a disclosure of the security breach to the Attorney General at the same time the security breach is disclosed to affected individuals or within 45-days after the person or business determines that there is a reasonable likelihood of harm to customers, whichever occurs first.

WHAT DATA IS COVERED?

Under § 4-110-103(7), personal information is covered, meaning an individual's first name or first initial and his or her last name in combination with any one or more of the following data elements when either the name or data element is not encrypted or redacted:

(1) social security number;

(2) driver's license number or Arkansas 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;

(4) medical information; and

(5) Biometric Data, which means data generated by automatic measurements of an individual's biological characteristics, including without limitation: fingerprints, faceprint, a retinal or iris scan, hand geometry, voiceprint analysis, DNA, or any other unique biological characteristic of an individual if the characteristics are used by the owner or licensee to uniquely authenticate the individual's identity when the individual accesses a system or account.

---

[8] Publicly available at: *Arkansas Code*, Title 4. Business and Commercial Law § 4-110-101, www.findlaw.com, http://codes.findlaw.com/ar/title-4-business-and-commercial-law/ar-code-sect-4-110-101.html (last visited June 12, 2019).

[9] Amendment publicly available at: *Arkansas State Legislature*, HB 1943 – To amend the Personal Information Protection Act; and to revise the definition of "Personal Information" in the Personal Information Protection Act, http://www.arkleg.state.ar.us/assembly/2019/2019R/Pages/BillInformation.aspx?measureno=HB1943 (last visited May 24, 2019).

WHAT CONSTITUTES A DATA BREACH?

Under § 4-110-103(1)(A)–(B), a data breach means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person or business.

A data breach does not include the good faith acquisition of personal information by an employee or agent of the person or business for the legitimate purposes of the person or business if the personal information is not otherwise used or subject to further unauthorized disclosure.

WHO MUST BE NOTIFIED?

Under § 4-110-105(a)(1)-(b), any resident of Arkansas and the owner or licensee of the information whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person must be notified.

WHEN MUST NOTICE BE SENT?

Under § 4-110-105(a)(2), notice must be sent in the most expedient time and manner possible and without unreasonable delay, consistent with the legitimate needs of law enforcements as provide by this statute.

Under § 4-110-105(b)(1), a person or business affected by a breach that does not own the personal information data must notify the owner or licensee that there has been a breach immediately following discovery if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

IN WHAT FORM AND MANNER MUST NOTICE BE SENT?

Under § 4-110-105(e), notice may be provided by one of the following methods:

(1) written notice;

(2) electronic mail notice if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001, as it existed on January 1, 2005; or

(3) substitute notice if the person demonstrates that the cost of providing notice would exceed $250,000; the affected class of person to be notified exceeds 500,000; or the person or business does not have sufficient contact information.

Substitute notice consists of:

(1) electronic mail notice when the person or business has an electronic mail address for the subject persons;

(2) conspicuous posting of the notice on the website of the person or business if the person or business maintains a website; and

(3) notification by a statewide media.

WHAT MUST THE NOTICE SAY?

There are no specific requirements. The notice must simply carry out its purpose of notifying affected individuals of the breach.

ARE THERE ANY EXEMPTIONS?

Under § 4-110-106, the provisions of this chapter do not apply to a person or business that is regulated by a state or federal law that provides greater protection to personal information and at least as thorough disclosure requirements for breaches of the security of personal information than that provided by this chapter.

Under § 4-110-105(f), a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this section shall be deemed to be in compliance with the notification requirements of this section if the person or business notifies affected persons in accordance with its policies in the event of a breach of the security system.

WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

Under § 4-110-108, any violation is enforced by the Attorney General under the provisions of § 4-88-101 *et seq.*

ARE THERE ANY DATA SECURITY REQUIREMENTS IMPOSED?

Under § 4-110-104(a), a person or business shall take all reasonable steps to destroy or arrange for the destruction of a customer's records within its custody or control containing personal information that is no longer to be retained by the person or business by shredding, erasing, or otherwise modifying the personal information in the records to make it unreadable or undecipherable through any means.

Under § 4-110-104(b), a person or business that acquires, owns, or licenses personal information about an Arkansas resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

Under § 23-61-113, all licensed insurers, health maintenance organizations, or other insuring health entities regulated by the commissioner, producers, and other persons licensed or required to be licensed, authorized or required to be authorized, or registered or required to be registered must provide notice of a data breach to the Insurance Commissioner in the same time and manner as § 4-110-105.

CALIFORNIA

STATUTE: Cal. Civ. Code §§ 1798.29,[10] 1798.80 *et seq.*[11]

WHO MUST COMPLY?

Under § 1798.29(a), any agency that owns or licenses computerized data that includes personal information shall comply, and under § 1798.82(a)-(b), a person or business that conducts business in California and that owns or licenses computerized data that includes personal information and a person or business that maintains computerized data that includes personal information that the person or business does not own.

Under § 1798.80, "business" means a sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the law of this state, any other state, the United States, or of any other country, or the parent or the subsidiary of a financial institution. The term includes an entity that disposes of records.

§ 1798.29 applies to governmental entities, whereas § 1798.80 *et seq.* applies to non-governmental entities.

WHAT DATA IS COVERED?

Under §§ 1798.29(g) and 1798.82(d), unencrypted personal information is covered. Further, encrypted personal information that was, or is reasonably believed to have been, acquired by an unauthorized person where the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person and the owner or licensee of that encrypted information has a reasonable belief that the encryption key or security credential could render that personal information readable or usable is covered.

Under § 1798.29(g) and § 1798.82(h), "personal information" is defined as:

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

(a) social security number;

(b) driver's license number or California identification card number;

[10] Publicly available at: *California Legislative Information*, www.leginfo.legislature.ca.gov, https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.29 (last visited June 12, 2019).
[11] Publicly available at: *California Legislative Information*, www.leginfo.legislature.ca.gov, https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=1798.80.&lawCode=CIV (last visited June 12, 2019).

(c) 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;

(d) medical information, meaning any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional;

(e) health insurance information, meaning an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records; or

(f) information or data collected through the use or operation of an automated license plate recognition system, as defined in § 1798.90.5.

(2) A user name or email address, in combination with a password or security question and answer that would permit access to an online account.

Under § 1798.80(e), "personal information" means any information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information.

"Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

WHAT CONSTITUTES A DATA BREACH?

Data breach means an unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency.

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

WHO MUST BE NOTIFIED?

Any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person must be notified, or, whose encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person and the agency that owns or licenses the encrypted

information has a reasonable belief that the encryption key or security credential could render that person information readable or useable.

The owner or licensee of the information of any breach of the security of the data must also be notified.

Any agency or person or business that is required to issue a security breach notification pursuant to § 1789.29 or § 1798.82 to more than 500 California residents as a result of a single breach shall electronically submit a sample copy of the security breach notification, excluding any personally identifiable information, to the Attorney General.

WHEN MUST NOTICE BE SENT?

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

Notice to the owner or licensee of data must be made immediately following discovery if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

IN WHAT FORM AND MANNER MUST NOTICE BE SENT?

Notice may be provided by one of the following methods:

(1) written notice;

(2) electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in § 7001 of Title 15 of the United States Code; or

(3) substitute notice, if the agency or person or business demonstrates that the cost of providing notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000, or the agency does not have sufficient contact information.

Substitute notice shall consist of:

(1) email notice when the agency or business has an email address for the subject persons;

(2) conspicuous posting, for a minimum of 30 days, of the notice on the agency or business' Internet Web site page, if the agency or person or business maintains one. For purposes of this subparagraph, conspicuous posting on the person's or business's Internet Web site means providing a link to the notice on the home page or the first significant page after entering the Internet Web site that is in larger type than the surrounding text, or in contrasting type, font, or color to the

surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks that call attention to the link; and

(3) notification to major statewide media, and for agencies, notice to the Office of Information Security within the Department of Technology.

If a username or email address, in combination with a password or security question and answer that would permit access to an online account is breached, and no other information was breached, the agency or person or business may comply by providing the security breach notification in electronic form or other form that directs the person whose personal information has been breached to promptly change his or her password and security question or answer, as applicable, or to take other steps appropriate to protect the online account with the agency and all other online accounts for which the person uses the same user name or email address and password or security question or answer.

If a breach involves the login credentials of an email account furnished by the person or business, notice by electronic mail will not comply. Instead, the agency or person or business can comply by providing notice by another method described or by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an Internet Protocol address or online location from which the person or resident knows the resident customarily accesses the account.

WHAT MUST THE NOTICE SAY?

Under §§ 1798.29(d) and 1798.82(d):

(1) Any security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described in paragraph (2) under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.

(a) The format of the notice shall be designed to call attention to the nature and significance of the information it contains.

(b) The title and headings in the notice shall be clearly and conspicuously displayed.

(c) The text of the notice and any other notice provided pursuant to this section shall be no smaller than 10-point type.

(2) The security breach notification shall include, at a minimum, the following information:

(a) The name and contact information of the reporting agency or reporting person or business subject to this section;

(b) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;

(c) If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice;

(d) Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided;

(e) A general description of the breach incident, if that information is possible to determine at the time the notice is provided;

(f) The toll-free telephone numbers and addresses of the major credit reporting agencies, if the breach exposed a social security number or a driver's license or California identification card number;

Under § 1798.82, if the person or business providing notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information that was either a social security number or driver's license number or California identification card number.

The security breach notification may also include any of the following:

(1) Information about what has been done to protect individuals whose information has been breached;

(2) Advice on steps that the person whose information has been breached may take to protect himself or herself.

ARE THERE ANY EXEMPTIONS?

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

Under § 1798.82(e), a covered entity under the federal Health Insurance Portability and Accountability Act of 1996 will be deemed to have complied with the notice requirements of § 1798.82(d) if it has complied completely with section 1340(f) of the federal Health Information Technology for Economic and Clinic Health Act (Public Law 111-5). However, this shall not be construed as exempting a covered entity from any other provision of this section.

An agency or a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information which is otherwise consistent with the timing requirements of these parts shall be deemed to be in compliance with the notification requirements of this section if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.

WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

Under § 1798.84, there is a private right of action available to recover damages for violations. Entities in violation of this title may also be enjoined. In addition, for a willful, intentional, or reckless violation of § 1798.83, dealing with disclosure to direct marketers, a customer may recover a civil penalty not to exceed $3,000 per violation; otherwise, the customer may recover a civil penalty of up to $500 per violation for a violation of § 1798.83.

ARE THERE ANY DATA SECURITY REQUIREMENTS IMPOSED?

A business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure. § 1798.81.5(b).

"Reasonable security practices" has not been codified, but in the California Data Breach Report 2012-2015, the California Attorney General states that "the 20 controls in the Center for Internet Security's critical security controls define a minimum level of information security that all organizations that collect or maintain personal information should meet. The failure to implement all the controls that apply to an organization's environment constitutes a lack of reasonable security." The Center for Internet Security's controls are available here: **https://www.cisecurity.org/controls/**.

ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

Yes, medical information statutes. Section 1280.15: Patient medical information; unlawful or unauthorized access or use; reporting period; administrative penalty. Any unlawful or unauthorized access to, or use or disclosure of, a patient's medical information constitutes a data breach.

Any individually identifiable information, in electronic or physical form, regarding a patient's medical history, mental or physical condition, or treatment constitutes personal information or data.

A clinic, health facility, home health agency, or hospice licensed pursuant to §§ 1205, 1250, 1725 or 1745 must comply.

Notification must be made within five days after detection of the breach, except as necessary for law enforcement purposes. Notification must also be made to state health authorities.

Additionally, on June 28, 2018, Governor Jerry Brown signed the California Consumer Privacy Act of 2018,[12] which will become effective January 1, 2020. The law, codified at Title 1.81.5 to Part 4 of Division 3 of the California Civil Code, mandates robust privacy protections for consumers, including the following:

(1) The right to know the categories and specific pieces of personal information collected from consumers, the categories of sources from which the personal information is collected, and the business purpose for collecting or sharing the personal information.

(2) The right to know whether personal information is sold or disclosed, and the categories of third parties with whom personal information is shared.

(3) The right to opt out of allowing a business to sell their personal information to third parties through a link on the company's website titled "Do Not Sell My Personal Information" (or, for consumers under 16, to have their personal information not sold unless they opt in, and for consumer under 13 years old, to have their personal information not sold unless the child's parent or guardian opts in).

(4) The right to access personal information (must be provided within 45 days of a request, subject to certain extensions), including the right to request the deletion of personal information, subject to certain exceptions.

(5) The right to equal service and price, even when exercising privacy rights. Companies are allowed, however, to charge consumers different prices or provide different levels of services, if those differences are directly related to the value provided to the consumer by the consumer's data. Additionally, companies can offer financial incentives for the collection/sale/deletion of personal information.

The California Consumer Privacy Act of 2018 will require companies subject to it to determine what personal data they are collecting from consumers, for what purpose, and to update their privacy policies every 12 months in order to make the disclosures to consumers required by the Act.

The Act can be enforced by the California Attorney General, subject to a 30 day cure period. A civil penalty of up to $7,500 per violation is provided for in the Act. In addition, the Act provides for a private right of action for consumers (individually or on a class-wide basis) with respect to sensitive personal information (which is more narrowly defined in the Act) if wrongfully accessed or disclosed as a result of the company's failure to implement and maintain required reasonable security protocols. Statutory damages (which, if sought, first require 30 days written notice by the consumer to the company, allowing the company to cure) range between $100 and $750 for California consumer per incident, or, if greater, actual damages (which do not require advance notice to the company) can be recovered, as well as injunctive relief. A consumer lawsuit must be noticed to the Attorney General within 30 days of filing, who can then prosecute

[12] Publicly available at: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375 (last visited June 12, 2019).

the action instead (but if the Attorney General does not prosecute within 6 months, the consumer can proceed with his/her lawsuit); instruct the consumer not to proceed with the lawsuit; or allow the consumer to proceed with the action (which is presumed if the Attorney General does not respond within 30 days).

COLORADO

STATUTE: Colo. Rev. Stat. §§ **6-1-713**; **6-1-713.5**; and 6-1-716 for non-governmental entities.[13] Colo. Rev. Stat § **24-73-103** for Governmental Entities.[14]

WHO MUST COMPLY?

Under § 716(2), a covered entity that maintains, owns, or licenses computerized data that includes personal information about a resident of Colorado must comply.

Under § 716(1)(b), a "covered entity" means a natural person, corporation, company, limited liability company, partnership, firm, association or other legal entity that maintains, owns, or licenses personal information in the course of the person's business, vocation, or occupation. But "covered entities" do not include any person acting as a third-party service provider.

Under § 24-73-103, a governmental entity that maintains, owns, or licenses computerized data that includes personal information about a resident of Colorado must comply.

"Governmental entity" means the state and any state agency or institution, including the judicial department, county, city and county, incorporated city or town, school district, special improvement district, authority, and every other kind of district, instrumentality, or political subdivision of the state organized pursuant to law. It includes entities governed by home rule charters. It does not include an entity acting as a third-party service provider, which is an entity that has been contracted to maintain, store, or process personal information on behalf of a governmental entity.

WHAT DATA IS COVERED?

Under § 716(2) and § 24-73-103(b), computerized data that includes personal information about a resident of Colorado is covered.

Under § 716(1)(g)(I)(A) and § 24-73-103(1)(g), "personal information" means a Colorado resident's first name or first initial and last name in combination with any one or more of the following data elements that relate to the resident, when the data elements are not encrypted, redacted, or secured by any other method rendering the name or the element unreadable or unusable:

(1) Social security number;

(2) Student, military, or passport identification number;

(3) Driver's license number or identification card number;

---

[13] Publicly available at: *Colorado Legal Resources*, www.lexisnexis.com, https://leg.colorado.gov/sites/default/files/documents/2018A/bills/2018a_1128_enr.pdf (last visited June 12, 2019). The amendments to the statute, discussed herein, will become effective September 1, 2018.

[14] *Id.*

(4) Medical information, defines as any information about a consumer's medical or mental health treatment or diagnosis by a health care professional;

(5) Health insurance identification number; or

(6) Biometric data, defined as unique biometric data generated from measurements or analysis of human body characteristics for the purpose of authenticating the individual when he or she accesses an online account.

"Personal information" also includes a Colorado resident's username or e-mail address, in combination with a password or security questions and answers, that would permit access to an online account.

Additionally, "personal information" includes a Colorado resident's account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to that account.

But, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.

WHAT CONSTITUTES A DATA BREACH?

Under § 716(1)(h) and § 24-73-103(1)(h), "security breach" refers to the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a covered entity.

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

Under §716(2)(g) and § 24-73-103(2)(d), the breach of encrypted or otherwise secured personal information must be disclosed in accordance with this section if the confidential process, encryption key, or other means to decipher the secured information was also acquired or was reasonably believed to have been acquired in the security breach.

WHO MUST BE NOTIFIED?

Under § 716(2) and § 24-73-103(2), affected Colorado residents must be notified.

Under § 716(2)(d) and § 24-73-103(2)(i), if a covered entity is required to notify more than 1,000 Colorado residents of a security breach pursuant to this section, the covered entity shall also notify, in the most expedient time possible and without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by the federal "Fair Credit Reporting Act," 15 U.S.C. § 1681a(p), of the anticipated date of the notification to the residents and the approximate number of residents who are to be notified.

Under §716(f)(I) and § 24-73-103(k)(i), the covered entity that must notify Colorado residents of a data breach pursuant to this section shall provide notice of any security breach to the Colorado Attorney General if the security breach is reasonably believed to have affected 500 Colorado residents or more, unless the investigation determines that the misuse of information about a Colorado resident has not occurred and is not likely to occur.

WHEN MUST NOTICE BE SENT?

Under § 716(2) and § 24-73-103(2), notice shall be made to Colorado residents, all consumer reporting agencies, and the Attorney general in the most expedient time possible and without unreasonable delay, but not later than thirty days after the date or determination that a security breach occurred, 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.

IN WHAT FORM AND MANNER MUST NOTICE BE SENT?

Under § 716(1)(f) and § 24-73-103(1)(f), notice means:

(1) Written notice to the postal address listed in the records of the covered entity;

(2) Telephonic notice;

(3) Electronic notice, if a primary means of communication by the covered entity with a Colorado resident is by electronic means or the notice provided is consistent with the provisions regarding electronic records and signatures set forth in the federal "Electronic Signatures in Global and National Commerce Act," 15 U.S.C. § 7001, *et seq.*, or

(4) Substitute Notice, if the covered entity required to provide notice demonstrates that the cost of providing notice will exceed $250,000, the affected class of persons to be notified exceeds 250,000 Colorado residents, or the covered entity does not have sufficient contact information to provide notice. Substitute notice shall consist of all of the following:

   (a) E-mail notice if the covered entity has e-mail addresses for the members of the affected class of Colorado residents;

   (b) Conspicuous posting of the notice on the website page of the covered entity if the covered entity maintains one; and

   (c) Notification to major statewide media.

WHAT MUST THE NOTICE SAY?

Under § 716(2)(a.2) and § 24-73-103(2)(b), in the case of a breach of personal information, notice to affected Colorado residents must include, but need not be limited to, the following information:

(1) The date, estimated date, or estimated date range of the security breach;

(2) A description of the personal information that was acquired or reasonably believed to have been acquired as part of the security breach;

(3) Information that the resident can use to contact the covered entity to inquire about the security breach;

(4) The toll-free numbers, addresses, and websites for consumer reporting agencies;

(5) The toll-free number, address, and website for the Federal Trade Commission; and

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

Additionally, under § 716(2)(a.3) and § 24-73-103(2)(c), if personal information has been misused, or is reasonably likely to be misused, then the covered or governmental entity shall, in addition to the notice otherwise required, and in the most expedient time possible and without unreasonable delay, but not later than thirty days after the date of determination that a security breach occurred, 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:

(1) Direct the person whose personal information has been breached to promptly change his or her password and security question or answer, as applicable, or to take other steps appropriate to protect the online account with the covered entity and all other online accounts for which the person whose personal information has been breached uses the same username or e-mail address and password or security question or answer.

(2) For log-in credentials of an e-mail account furnished by the covered entity, the covered entity shall not comply with this section by providing the security breach notification to that e-mail address, but may instead comply with this section by providing notice through other methods, as defined in subsection (1)(f) of this section, or by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an internet protocol address or online location from which the covered entity knows the resident customarily accesses the account.

Under § 716(2)(a.4), a breach of encrypted or otherwise secured personal information must be disclosed in accordance with the provisions of § 716(2) if the confidential process, encryption key, or other means to decipher the secured information was also acquired in the security breach or was reasonably believed to have been acquired.

Furthermore, under § 716(2)(a.5), a covered entity that is required to provide notice to affected Colorado residents pursuant to the provisions of § 716(2) is prohibited from charging the cost of providing such notice to such residents.

ARE THERE ANY EXEMPTIONS?

Under § 716(2)(c) and § 24-73-103(2)(h), notice may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation and the law enforcement agency has notified the covered entity that conducts business in Colorado not to send notice required by this section. Notice required by this section must be made in good faith, in the most expedient time possible and without unreasonable delay but not later than 30 days after the law enforcement agency determines that notification will no longer impede the investigation and has notified the covered entity that conducts business in Colorado that it is appropriate to send the notice required by this section.

Under §716(2)(d); covered entities subject to Title V of the Gramm-Leach-Bliley Act are exempt from notifying all consumer reporting agencies.

Under §716(3)(a) and § 24-73-103(3)(a), if a covered entity or governmental entity maintains its own notification procedures as part of an information security policy for the treatment of personal information and whose procedures are otherwise consistent with the timing requirements of this section, the covered entity is in compliance with the notice requirements if the covered entity notifies affected Colorado residents in accordance with its policies in the event of a security breach; except that notice to the attorney general is still required.

Under §716(3)(b) and § 24-73-103(3)(b), a covered entity that is regulated by state or federal law and that maintains procedures for a security breach pursuant to the laws, rules, regulations, guidances, or guidelines established by its state or federal regulator is in compliance with this section; except that notice to the attorney general is still required. In the event of a conflict in timing requirements for notice, the requirement with the shortest notice period controls.

WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

Under § 716(4), the Attorney General may bring an action in law or in equity to address violations of this section, and for other relief that may be appropriate to ensure compliance with this section or to recover direct economic damages resulting from a violation, or both.

Additionally, § 716(5) and § 24-73-103(5) confer broad criminal enforcement authority upon the Attorney General. Specifically, upon receiving notice of a breach, and with either a request from the governor to prosecute a particular case, or with the approval of the district attorney with jurisdiction to prosecute cases in the judicial district where a case could be brought, the attorney general has the authority to prosecute any criminal violations of section 18-5.5-102 regarding cybercrimes.

Under § 24-73-103(4), the attorney general may bring an action for injunctive relief to enforce the provisions of § 24-73-103.

ARE THERE ANY DATA SECURITY REQUIREMENTS IMPOSED?

Under § 713.5(1), a covered entity that maintains, owns, or licenses personal identifying information of an individual residing in the state shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal identifying information and the nature and size of the business and its operations.

Under § 713.5(2), unless a covered entity agrees to provide its own security protection for the information it discloses to a third-party service provider, the covered entity shall require that the third-party service provider implement and maintain reasonable security procedures and practices that are:

(1) appropriate to the nature of the personal identifying information disclosed to the third-party service provider; and

(2) reasonably designed to help protect the personal identifying information from unauthorized access, use, modification, disclosure, or destruction.

Under § 713.5(3), a disclosure of personal identifying information does not include disclosure of information to a third party under circumstances where the covered entity retains primary responsibility for implementing and maintaining reasonable security procedures and practices appropriate to the nature of the personal identifying information and the covered entity implements and maintains technical controls that are reasonably designed to:

(1) help protect the personal identifying information from unauthorized access, use, modification, disclosure, or destruction; or

(2) effectively eliminate the third party's ability to access the personal identifying information, notwithstanding the third party's physical possession of the personal identifying information.

Under § 713.5(4), a covered entity that is regulated by state or federal law and that maintains procedures for protection of personal identifying information pursuant to the laws, rules, regulations, guidances, or guidelines established by its state or federal regulator is in compliance with this section.

ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

None.

CONNECTICUT

STATUTE: Conn. Gen. Stat. §§ **36a-701a**,[15] **36a-701b**,[16] **38a-999b**,[17] **4e-70**,[18]

WHO MUST COMPLY?

Under § 36a-701b(b)(1), any person who conducts business in Connecticut, and who, in the ordinary course of such person's business, owns, licenses or maintains computerized data that includes personal information must comply.

Under § 36a-701b(c), any person that maintains computerized data that includes personal information that the person does not own must comply.

WHAT DATA IS COVERED?

Under § 36a-701b(a), personal information is covered. "Personal information" means an individual's first name or first initial and last name in combination with any one, or more, of the following data: (A) social security number; (B) driver's license number or state identification card number; or (C) credit or debit card number, or (D) financial account number in combination with any required security code, access code or password that would permit access to an individual's such financial account.

"Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media.

WHAT CONSTITUTES A DATA BREACH?

Under § 36a-701b(a), a data breach means unauthorized access to or unauthorized acquisition of electronic files, media, databases or computerized data containing personal information when access to the personal information has not been secured by encryption or by any other methods or technology that renders the personal information unreadable or unusable.

WHO MUST BE NOTIFIED?

Under § 36a-701b(b)(1), any resident of Connecticut whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person through such breach of security must be notified. Under § 36a-701b(b)(2), the Attorney General must be notified. Under § 36a-701b(c), the owner or licensee of the information of any breach of security of the data

[15] Publicly available at: *2016 Connecticut General Statutes Title 36a*, www.law.justia.com, https://law.justia.com/codes/connecticut/2016/title-36a/chapter-669/section-36a-701/ (last visited June 12, 2019).
[16] Publicly available at: 2015 *Connecticut General Statutes Title 36a*, www.law.justia.com, https://law.justia.com/codes/connecticut/2015/title-36a/chapter-669/section-36a-701b (last visited June 12, 2019).
[17] Publicly available at: 2015 *Connecticut General Statutes Title 38a*, www.law.justia.com, https://law.justia.com/codes/connecticut/2015/title-38a/chapter-705/section-38a-999b (last visited June 12, 2019).
[18] Publicly available at: 2015 *Connecticut General Statutes Title 4e*, www.law.justia.com, https://law.justia.com/codes/connecticut/2015/title-4e/chapter-62a/section-4e-70 (last visited June 12, 2019).

must be notified if personal information was breached, or is reasonably believed to have been breached.

WHEN MUST NOTICE BE SENT?

Under § 36a-701b(b)(1), notice shall be made without unreasonable delay, but no later than ninety days after the discovery of such breach, unless a shorter time is required under federal law, subject to the provisions of subsection (d) of this section and the completion of an investigation by such person to determine the nature and scope of the incident, to identify the individuals affected, or to restore the reasonable integrity of the data system.

IN WHAT FORM AND MANNER MUST NOTICE BE SENT?

Under § 36a-701b(e), notice may be provided by one of the following methods: (1) written notice; (2) telephone notice; (3) electronic notice, provided such notice is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001; or (4) substitute notice, provided such person demonstrates that the cost of providing notice in accordance with subdivision (1), (2) or (3) of this subsection would exceed $250,000, that the affected class of subject persons to be notified exceeds 500,000 persons, or that the person does not have sufficient contact information.

Substitute notice shall consist of the following: (A) electronic mail notice when the person has an electronic mail address of the affected persons; (B) conspicuous posting of the notice on the website of the person if the person maintains one; and (C) notification to major state-wide media, including newspapers, radio and television.

WHAT MUST THE NOTICE SAY?

There is no required format. The notice must simply carry out its purpose of notifying affected individuals of the breach. In addition, the covered entity providing notice must offer each resident whose Social Security Number was compromised as the result of a breach appropriate identity theft prevention and mitigation services. Such services shall be provided at no cost to such resident for a period of not less than twelve months. Such person shall provide all information necessary for such resident to enroll in such service or services and shall include information on how such resident can place a credit freeze on such resident's credit file. Conn. Gen. Stat. § 36a-701b(b)(2)(B).

ARE THERE ANY EXEMPTIONS?

Under §36a-701b(b)(1), notification shall not be required if, after an appropriate investigation and consultation with relevant federal, state and local agencies responsible for law enforcement, the person reasonably determines that the breach will not likely result in harm to the individuals whose personal information has been acquired or accessed.

Under § 36a-701b(d), any notification required by this section shall be delayed for a reasonable period of time if a law enforcement agency determines that the notification will impede a

criminal investigation and such law enforcement agency has made a request that the notification be delayed. Any such delayed notification shall be made after such law enforcement agency determines that notification will not compromise the criminal investigation and so notifies the person of such determination.

Under § 36a-701b(f), any person that maintains their own security breach procedures as part of an information security policy for the treatment of personal information and which otherwise complies with the timing requirements of this section, shall be deemed to be in compliance with the security breach notification requirements of this section, provided such person notifies, as applicable, residents of this state, owners or licensees in accordance with such person's policies in the event of a breach of security and in the case of notice to a resident, such person also notifies the Attorney General not later than the time when notice is provided to the resident.

Any person that maintains such security breach procedure pursuant to the rules, regulations, procedures or guidelines established by the primary or functional regulator, as defined in 15 U.S.C. § 6809(2), shall be deemed to be in compliance with the security breach notification requirements of this section, provided (1) such person notifies, as applicable, such residents of this state, owners, and licensees required to be notified under and in accordance with the policies or the rules, regulations, procedures or guidelines established by the primary or functional regulator in the event of a breach of security, and (2) if notice is given to a resident of this state in accordance with subdivision (1) of this subsection regarding a breach of security, such person also notifies the Attorney General not later than the time when notice is provided to the resident.

WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

Failure to comply with the requirements of this section shall constitute an unfair trade practice for purposes of § 42-110b and shall be enforced by the Attorney General.

The Attorney General may investigate any violation of this section. If the Attorney General finds that a contractor has violated or is violating any provision of this section, the Attorney General may bring a civil action in the Superior Court for the Judicial District of Hartford under this section in the name of the State against such contractor. Nothing in this section shall be construed to create a private right of action. Under § 36a-701(b)(2)(B), persons who must comply with the law shall offer to each resident whose personal information was breached or is reasonably believed to have been breached, appropriate identity theft prevention services and, if applicable, identity theft mitigation services at no cost to such resident for a period of not less than twelve months. Such persons shall provide all information necessary for such resident to enroll in such service or services and shall include information on how such resident can place a credit freeze on such resident's credit file.

ARE THERE ANY DATA SECURITY REQUIREMENTS IMPOSED?

Under § 4e-70, state contractors shall require the contractor to, at a minimum, do the following:

(1) At its own expense, protect from a confidential information breach any and all confidential information that it comes to possess or control, wherever and however stored or maintained;

(2) Implement and maintain a comprehensive data-security program for the protection of confidential information. The safeguards contained in such program shall be consistent with and comply with the safeguards for protection of confidential information as set forth in all applicable federal and state law and written policies of the state contained in the agreement. Such data-security program shall include, but not be limited to, the following: (A) A security policy for contractor employees related to the storage, access and transportation of data containing confidential information; (B) reasonable restrictions on access to records containing confidential information, including the area where such records are kept and secure passwords for electronically stored records; (C) a process for reviewing policies and security measures at least annually; and (D) an active and ongoing employee security awareness program that is mandatory for all employees who may have access to confidential information provided by the state contracting agency that, at a minimum, advises such employees of the confidentiality of the information, the safeguards required to protect the information and any applicable civil and criminal penalties for noncompliance pursuant to state and federal law;

(3) Limit access to confidential information to authorized contractor employees and authorized agents of the contractor, for authorized purposes as necessary for the completion of the contracted services or provision of the contracted goods;

(4) Maintain all electronic data constituting confidential information obtained from state contracting agencies: (A) In a secure server; (B) on secure drives; (C) behind firewall protections and monitored by intrusion detection software; (D) in a manner where access is restricted to authorized employees and their authorized agents; and (E) as otherwise required under state and federal law;

(5) Implement, maintain and update security and breach investigation procedures that are appropriate given the nature of the information disclosed and that are reasonably designed to protect the confidential information from unauthorized access, use, modification, disclosure, manipulation or destruction;

(6) Notify the state contracting agency and the Attorney General as soon as practical after the contractor becomes aware of or has reason to believe that any confidential information that the contractor possesses or controls has been subject to a confidential information breach;

(7) Immediately cease all use of the data provided by the state contracting agency or developed internally by the contractor pursuant to a written agreement with the state if so directed by the state contracting agency; and

(8) In accordance with the proposed timetable established pursuant to subdivision (1) of subsection (e) of this section, submit to the office of the Attorney General and the state contracting agency either (A) a report detailing the breach or suspected breach, including a plan to mitigate the effects of any breach and specifying the steps taken to ensure future breaches do not occur, or (B) a report detailing why, upon further investigation, the contractor believes no breach has occurred. Any report submitted under this subdivision shall be considered information given in confidence and not required by statute, under subparagraph (B) of subdivision (5) of subsection (b) of section 1-210.

Under §38a-999b, health insurers shall implement and maintain a comprehensive information security program to safeguard the personal information of insureds and enrollees that is compiled or maintained by such company. Such security program shall be in writing and contain administrative, technical and physical safeguards that are appropriate to (A) the size, scope and type of business of such company, (B) the amount of resources available to such company, (C) the amount of data compiled or maintained by such company, and (D) the need for security and confidentiality of such data.

Each company shall update such security program as often as necessary and practicable but at least annually and shall include in such security program:

(1) Secure computer and Internet user authentication protocols that include, but are not limited to, (i) control of user identifications and other identifiers, (ii) multifactor authentication that includes a reasonably secure method of assigning and selecting a password or the use of unique identifier technologies such as biometrics or security tokens, (iii) control of security passwords to ensure that such passwords are maintained in a location and format that do not compromise the security of personal information, (iv) restriction of access to only active users and active user accounts, and (v) the blocking of access after multiple unsuccessful attempts to gain access to data compiled or maintained by a company;

(2) Secure access control measures that include, but are not limited to, (i) restriction of access to personal information to only those individuals who require such data to perform their job duties, (ii) assignment, to each individual with computer and Internet access to data compiled or maintained by such company, of passwords that are not vendor-assigned default passwords and that require resetting not less than every six months and of unique user identifications, that are designed to maintain the integrity of the security of the access controls, (iii) encryption of all personal information while being transmitted on a public Internet network or wirelessly, (iv) encryption of all personal information stored on a laptop computer or other portable device, (v) monitoring of such company's security systems for breaches of security, (vi) for personal information that is stored or accessible on a

system that is connected to the Internet, reasonably up-to-date software security protection that can support updates and patches, including, but not limited to, firewall protection, operating system security patches and malicious software protection, and (vii) employee education and training on the proper use of the company's security systems and the importance of the security of personal information;

(3) Designation of one or more employees to oversee such security program and the maintenance of such security program;

(4) (i) Identification and assessment of reasonably foreseeable internal and external risks to the security, confidentiality or integrity of any electronic, paper or other records that contain personal information, (ii) evaluation and improvement where necessary of the effectiveness of the current safeguards for limiting such risks, including, but not limited to, (I) ongoing employee training, (II) employee compliance with security policies and procedures, and (III) means for detecting and preventing security system failures, and (iii) the upgrade of safeguards as necessary to limit risks;

(5) Development of employee security policies and procedures for the storage of, access to, transport of and transmittal of personal information off-premises;

(6) Imposition of disciplinary measures on employees for violating security policies or procedures or other provisions of the comprehensive information security program;

(7) Prevention of terminated, inactive or retired employees from accessing personal information;

(8) Oversight of third parties with which such company enters into contracts or agreements that have or will have access to personal information compiled or maintained by the company, by (i) selecting third parties that are capable of maintaining appropriate safeguards consistent with this subsection to protect such personal information, and (ii) requiring such third parties by contract or agreement to implement and maintain such safeguards;

(9) Reasonable restrictions on physical access to personal information in paper format and storage of such data in locked facilities, storage areas or containers;

(10) Review of the scope of the secure access control measures at least annually or whenever there is a material change in the company's business practices that may affect the security, confidentiality or integrity of personal information;

(11) Mandatory post-incident review by the company following any actual or suspected breach of security, and documentation of actions the company takes in response to such breach, including any changes the company makes to its business practices relating to the safeguarding of personal information; and

(12) Any other safeguards the company believes will enhance its comprehensive information security program.

ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

State Contractors. Under § 4e-70, contractors who receive confidential information are required to take certain steps to protect the information and notify the state contracting agency and the Attorney General after the contractor becomes aware of, or has reason to believe that, any confidential information that the contractor possesses or controls has been subject to a confidential information breach. The requirements are in addition to § 36a-701b.

Insurance. Under § 38a-999b of the Connecticut Insurance Information and Privacy Protection Act, a breach of security has the same meaning as section 36a-701b, but personal information is expanded to include: protected health information as defined in 45 CFR § 160.103, as amended from time to time; a taxpayer identification number; an alien registration number; a government passport number; a demand deposit account number; a savings account number; or unique biometric data, such as a fingerprint, a voice print, a retina or an iris image, or other unique physical representations.

Under § 38-a-999b(e), each company that discovers an actual or suspected breach of security shall (1) comply with the notice requirements of § 36a-701(b), (2) be subject to the penalty set forth in subsection (g) of § 36a-701b for failure to comply, and (3) offer appropriate identity theft prevention services and, if applicable, identity theft mitigation services.

The Insurance Commissioner enforces the provisions of § 38a-999b(b) – (d), inclusive, of this section.

DELAWARE

STATUTE: Del. Code 6, §§ 12B-100, *et seq.*[19]

WHO MUST COMPLY?

Under § 12B-102(a), any person who conducts business in Delaware and who owns or licenses computerized data that includes personal information shall provide notice of any breach of security following determination of the breach of security to any resident of Delaware whose personal information was breached or is reasonably believed to have been breached, unless, after an appropriate investigation, the person reasonably determines that the breach of security is unlikely to result in harm to the individuals whose personal information has been breached.

Under § 12B-101, "person" means an individual; corporation; business trust; estate trust; partnership; limited liability company; association; joint venture; government; governmental subdivision, agency, or instrumentality; public corporation; or any other legal or commercial entity.

Under § 12B-102(b), a person that maintains computerized data that includes personal information that the person does not own or license shall give notice to and cooperate with the licensee of the information of any breach of security immediately following determination of the breach of security. For purposes of this section, "cooperation" includes sharing with the owner or licensee information relevant to the breach.

WHAT DATA IS COVERED?

Under § 12B-101(7)a, "personal information" means a Delaware resident's first name or first initial and last name in combination with any 1 or more of the following data elements that relate to that individual:

(1) Social Security number;

(2) Driver's license number or state or federal 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 a resident's financial account.

(4) 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.

[19] Publicly available at: *State of Delaware – Title 6*, http://delcode.delaware.gov/title6/c012b/index.shtml (last visited June 12, 2019). Delaware has enacted amendments to its data breach notification statute that, among other things, add a definition of "encrypted" and modify the definition of "personal information" and impose a duty on "any person who conducts business in Delaware and owns, licenses, or maintains personal information" to maintain procedures to safeguard such information." Those amendments took effect on April 14, 2018. Del. HB 180, Gen. Assemb.

(6) Medical history, medical treatment by a healthcare professional, diagnosis of mental or physical condition by a health care professional, or deoxyribonucleic acid (DNA) profile.

(7) Health insurance policy number, subscriber identification number, or any other 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.

Additionally, under § 12B-101(7)b, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely-distributed media.

WHAT CONSTITUTES A DATA BREACH?

Under § 12B-101(1)a, a "breach of security" means "the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information. Good faith acquisition of personal information by an employee or agent of any person for the purposes of such person is not a breach of security, provided that the personal information is not used for an unauthorized purpose or subject to further unauthorized disclosure."

Furthermore, under § 12B-101(1)b, "[t]he unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information is not a breach of security to the extent that personal information contained therein is encrypted, unless such unauthorized acquisition includes, or is reasonably believed to include, the encryption key and the person that owns or licenses the encrypted information has a reasonable belief that the encryption key could render that personal information readable or useable."

WHO MUST BE NOTIFIED?

Under § 12B-102(a), any resident of Delaware whose personal information was breached or is reasonably believed to have been breached, unless, after an appropriate investigation, the complying person reasonably determines that the breach of security is unlikely to result in harm to the individuals whose personal information has been breached.

Furthermore, under § 12B-102(b), a person that maintains computerized data that includes personal information that the person does not own or license shall give notice to and cooperate with the owner or licensee of the information of any breach of immediately following determination of the breach of security. For purposes of this subsection, "cooperation" includes sharing with the owner or licensee information relevant to the breach.

Under § 12B-102(d), if the affected number of Delaware residents to be notified is over 500 residents, the Attorney General of Delaware must also be notified.

WHEN MUST NOTICE BE SENT?

Under § 12B-102(c), notice must be made must be made without unreasonable delay but not later than sixty days after determination of the breach of security, except when:

(1) A shorter time is required under federal law.

(2) A law enforcement agency determines that the notice will impede a criminal investigation and such law enforcement agency has made a request of the person that the notice be delayed. Any such delayed notice must be made after such law enforcement agency determines that notice will not compromise the criminal investigation and so notifies the person of such determination.

(3) When a person otherwise required to provide notice, could not, through reasonable diligence, identify within 60 days that the personal information of certain residents of Delaware was included in a breach of security, such person must provide the notice required by this title to such residents as soon as practicable after the determination that the breach of security included the personal information of such residents, unless such person provides or has provided substitute notice in accordance with § 12B-101(5)d of this title.

IN WHAT FORM AND MANNER MUST NOTICE BE SENT?

Under § 12B-101(5), notice may be provided by one of the following methods:

(1) Written notice;

(2) Telephonic notice;

(3) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in § 7001 of Title 15 of the United States Code, or if the person's primary means of communication with the resident is by electronic means; or

(4) Substitute notice, if the person required to provide notice under this chapter demonstrates that the cost of providing notice will exceed $75,000, or that the affected number of Delaware residents to be notified exceeds 100,000 residents, or that the person does not have sufficient contact information to provide notice.

Substitute notice consists of all of the following:

(1) Electronic notice if the person has email addresses for the members of the affected class of Delaware residents; unless the breach of security involves a username and address, in combination with a password or security question and answer that would permit access to an online account, in which any other form of notice must be provided, or by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an

Internet Protocol address or online location from which the person knows the resident customarily accesses the account.

(2) conspicuous posting of the notice on the web site page of the person, if the person maintains one or more website pages; or

(3) notice to major statewide media, including newspapers, radio, and television and publication on the major social media platforms of the person providing notice.

WHAT MUST THE NOTICE SAY?

No specific requirements. The notice must simply carry out its purpose of notifying affected individuals of the breach.

Under § 12B-102(e), if a breach of security includes a Social Security Number, the person shall offer to each resident, whose personal information, including Social Security number, was breached or is reasonably likely to have been breached, credit monitoring services at no cost to such resident for a period of one year. The person must provide all information necessary for such resident to enroll in such services and shall not include information on how such resident can place a credit freeze on such resident's credit file. Such services are not required if, after an appropriate investigation, the person reasonably determines that the breach of security is unlikely to result in harm to the individuals whose personal information has been breached.

ARE THERE ANY EXEMPTIONS?

Under § 12B-102(c), notice required by this chapter may be delayed if a law-enforcement agency determines that the notice will impede a criminal investigation.

The notification requirements do not apply if the exposed personal information is encrypted, unless such unauthorized acquisition includes, or is reasonably believed to include, the encryption key and the person that owns or licenses the encrypted information has a reasonable belief that the encryption key could render that personal information readable or useable.

"Encrypted" means personal information that is rendered unusable, unreadable, or indecipherable through a security technology or methodology generally accepted in the field of information security. § 12B-101(3).

"Encryption key" means the confidential key or process designed to render the encrypted personal information useable, readable, and decipherable. § 12B-101(4).

Under § 12B-103(a), a person that maintains its own notice procedures as part of an information security policy for the treatment of personal information, and whose procedure are otherwise consistent with the timing requirements of this chapter is deemed to be in compliance with the notice requirements of this chapter if the person notifies affected Delaware residents in accordance with its policies in the event of a breach of security.

Under § 12B-103(b), a person that is regulated by state or federal law, including the Health Insurance Portability and Accountability Act of 1996 (HIPPA) and the Gramm Leach Bliley Act

and that maintains procedures for a breach of security pursuant to the laws, rules, regulations, guidances, or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance with this chapter if the person notifies affected Delaware residents in accordance with the maintained procedures when a breach of security occurs.

WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

Under §12B-104(a), only the Attorney General may bring an action in law or equity to address the violations of this chapter and for other relief that may be appropriate to ensure proper compliance with this chapter or to recover direct economic damages resulting from a violation, or both. The provisions of this chapter are not exclusive and do not relieve a person subject to this chapter from compliance with all other applicable provisions of law.

Furthermore, under §12B-104(b), nothing in Delaware's date breach notification statute modifies any right which a person may have at common law, by statute, or otherwise.

ARE THERE ANY DATA SECURITY REQUIREMENTS IMPOSED?

Under § 12b-100, any person who conducts business in this state and owns, licenses, or maintains personal information shall implement and maintain reasonable procedures and practices to prevent the unauthorized acquisition, use, modification, disclosure, or destruction of personal information collected or maintained in the regular course of business.

ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

None.

DISTRICT OF COLUMBIA

STATUTE: D.C. Code §§ 28-3851 *et seq.*[20]

WHO MUST COMPLY?

Under § 28-3852(a), covered entities include 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.

Under § 28-3852(b), 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 must also comply.

WHAT DATA IS COVERED?

Under § 28-3852(a) and (b), personal information is covered. Under § 28-3851(3)(A), "personal information" means an individual's first name or first initial and last name, or phone number, or address, and any one or more of the following data elements:

(1) social security number;

(2) driver's license number or District of Columbia Identification Card number; or

(3) credit card number or debit card number; or

(4) 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.

The term "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

WHAT CONSTITUTES A DATA BREACH?

Under § 28-3851(1), a data breach 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.

A data breach does not include a good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business if the personal information is not used improperly or subject to further unauthorized disclosure. Further, acquisition of data that has been rendered secure, so as to be unusable by an unauthorized third party, shall not be deemed to be a breach of the security of the system.

[20] Publicly available at: *District of Columbia Official Code*, www.dccouncil.us, http://dccode.elaws.us/code?no=28-38%7CII (last visited June 12, 2019).

WHO MUST BE NOTIFIED?

Under § 28-3852(a), any District of Columbia resident whose personal information was included in the breach must be notified.

Under § 28-3852(b), the owner or licensee of the information compromised in any breach must be notified.

Under § 28-3852(c), if any person or entity is required to notify more than 1,000 persons of a breach of security, the person shall also notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by § 603(p) of the Fair Credit Reporting Act (15 U.S.C. §1681a(p)), of the timing, distribution, and content of the notices. However, the person or entity is not required to provide to the consumer reporting agency the names or other personal identifying information of breach notice recipients.

WHEN MUST NOTICE BE SENT?

Under § 28-3852(a), the notification must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, and without any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

Under § 28-3852(b), notice to an owner or licensee of compromised data shall be made in the most expedient time possible following discovery of a breach.

Under § 2803852(c), if any person or entity is required to notify consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, the person shall notify the consumer credit reporting agencies without unreasonable delay.

IN WHAT FORM AND MANNER MUST NOTICE BE SENT?

Under § 28-3851(2), notice may be sent through any of the following methods:

(1) written notice;

(2) electronic notice, if the customer has consented to receipt of electronic notice consistent with the provisions regarding electronic records and signatures set forth in the Electronic Signatures in Global and National Commerce Act; or

(3) substitute notice, if the person or business demonstrates that the cost of providing notice to person subject to this subchapter would exceed $50,000, that the number of persons to receive notice under this subchapter exceeds 100,000, or that the person or business does not have sufficient contact information.

Substitute notice shall consist of all of the following:

(1) email notice when the person or business has an email address for the subject person;

(2) conspicuous posting of the notice on the website page of the person or business if the person or business maintains one; and

(3) notice to major local and, if applicable, national media.

WHAT MUST THE NOTICE SAY?

No specific requirements. The notice must simply carry out its purpose of notifying affected individuals of the breach.

ARE THERE ANY EXEMPTIONS?

Under § 28-3852(c), covered persons or entities required to notify consumer reporting agencies of a breach pursuant to Title V of the Gramm-Leach-Bliley Act are not required to also notify consumer reporting agencies pursuant to D.C.'s statute.

Under § 28-3852(d), the notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation but shall be made as soon as possible after the law enforcement agency determines that the notification will not compromise the investigation.

Under § 28-3852(e), a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of § 28-3852 shall be deemed to be in compliance with the notification requirements of this section if the person or business provides notice, in accordance with its policies, reasonably calculated to give actual notice to persons to whom notice is otherwise required to be given under this subchapter. Notice under this section may be given by electronic mail if the person or entity's primary method of communication with the resident is by electronic means.

Under § 28-3852(g), a person or entity who maintains procedures for a breach notification system under Title V of the Gramm-Leach-Bliley Act (15 U.S.C. § 6801 *et seq.*), and provides notice in accordance with the Act, and any rules, regulations, guidance and guidelines thereto, to each affected resident in the event of a breach, shall be deemed to be in compliance with this section.

WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

Under § 28-3853(a), any District of Columbia resident injured by a violation of this subchapter may institute a civil action to recover actual damages, the costs of the action, and reasonable attorney's fees. Actual damages shall not include dignitary damages, including pain and suffering.

Under § 28-3853(b), the Attorney General may petition the Superior Court of the District of Columbia for temporary or permanent injunctive relief and for an award of restitution for property lost or damages suffered by District of Columbia residents. The Attorney General may recover a civil penalty not to exceed $100 for each violation, the costs of the action, and

reasonable attorney's fees. Each failure to provide a District of Columbia resident with notification in accordance with this section shall constitute a separate violation.

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

ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

None.

FLORIDA

STATUTE: Fla. Stat. §§ 501.171,[21] 282.0041,[22] 282.318(2)(i).[23]

WHO MUST COMPLY?

Under § 501.171(4), covered entities must comply. Under § 501.171(1)(b), "covered entity" means a sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity that acquires, maintains, stores, or uses personal information. For purposes of the notice requirements, the term includes a governmental entity.

Under § 501.171(6), in the event of a breach of a security system maintained by a third-party agent, such third-party agent shall notify the covered entity of the breach of security. Upon receiving notice, the covered entity shall provide notices under § 501.171(3) and (4).

WHAT DATA IS COVERED?

Under § 501.171(4), personal information is covered. Under § 501.171(1)g, "personal information" consists of an individual's first name or first initial and last name in combination with any one or more of the following data elements for that individual:

(1) social security number;

(2) driver's license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity;

(3) a financial account number or credit or debit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual's financial account;

(4) any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or

(5) an individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual.

"Personal information" also means a user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account.

---

[21] Publicly available at: *The 2017 Florida Statutes*, www.leg.state.fl.us, http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=0500-0599/0501/Sections/0501.171.html (last visited June 12, 2019).

[22] Publicly available at: *The 2017 Florida Statutes*, www.leg.state.fl.us, http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=0200-0299/0282/Sections/0282.0041.html (last visited June 12, 2019).

[23] Publicly available at: *The 2017 Florida Statutes*, www.leg.state.fl.us, http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=0200-0299/0282/Sections/0282.318.html (last visited June 12, 2019).

"Personal information" does not include information about an individual that has been made publicly available by a federal, state, or local governmental entity. The term also does not include information that is encrypted, secured, or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable.

WHAT CONSTITUTES A DATA BREACH?

Under § 501.171(1)(a), a breach means unauthorized access of data in electronic form containing personal information. Good faith access of personal information by an employee or agent of the covered entity does not constitute a breach of security, provided that the information is not used for a purpose unrelated to the business or subject to further unauthorized use.

WHO MUST BE NOTIFIED?

Under § 501.171(4)(a), a covered entity shall give notice to each individual in this state whose personal information was, or the covered entity reasonably believes to have been, accessed as a result of the breach.

A covered entity shall provide notice to the Department of Legal Affairs of any breach of security affecting 500 or more individuals in this state.

Under § 501.171(5), if a covered entity discovers circumstances requiring notice pursuant to this section of more than 1,000 individuals at a single time, the covered entity shall also notify, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in the Fair Credit Reporting Act (15 U.S.C. § 1681a(p)).

WHEN MUST NOTICE BE SENT?

Under § 501.171(4)(a), notice must be sent as expeditiously as practicable and without unreasonable delay, taking into account the time necessary to allow the covered entity to determine the scope of the breach of security, to identify individuals affected by the breach, and to restore the reasonable integrity of the data system that was breached but no later than 30 days after the determination of a breach or reason to believe a breach occurred.

Notice to the Department of Legal Affairs must be provided as expeditiously as practicable, but no later than 30 days after the determination of the breach or reason to believe a breach occurred. A covered entity may receive 15 additional days to provide notice as required by § 501.171(4) if good cause for delay is provided in writing to the department within 30 days after determination of the breach or reason to believe a breach occurred.

Under § 501.171(5), consumer reporting agencies shall be notified without unreasonable delay.

Under § 501.171(6), third-party agents shall notify covered entities of a breach as expeditiously as practicable, but no later than 10 days following the determination of the breach of security or reason to believe the breach occurred.

IN WHAT FORM AND MANNER MUST NOTICE BE SENT?

Under § 501.171(4), notice may be provided by one of the following methods:

(1) written notice sent to the mailing address of the individual in the records of the covered entity

(2) e-mail notice sent to the e-mail address of the individual in the records of the covered entity;

Additionally, under § 501.171(4)(f), a covered entity required to provide notice to an individual may provide substitute notice in lieu of direct notice if such direct notice is not feasible because the cost of providing notice would exceed $250,000, because the affected individuals exceed 500,000 persons, or because the covered entity does not have an e-mail address or mailing address for the affected individuals. Substitute notice shall include the following:

(1) a conspicuous notice on the Internet website of the covered entity if the covered entity maintains a website; and

(2) notice in print and to broadcast media, including major media in urban and rural areas where the affected individuals reside.

WHAT MUST THE NOTICE SAY?

Under § 501.171(4)(e), the notice shall include:

(1) the date, estimated date, or estimated date range of the breach of security;

(2) a description of the personal information that was accessed or reasonably believed to have been accessed as part of the breach of security; and

(3) information that the individual can use to contact the covered entity to inquire about the breach of security and the personal information that the covered entity maintained about the individual.

The written notice to the Department of Legal Affairs 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 required under subsection [§ 501.171(4)] or an explanation of the other actions taken pursuant to [§ 501.171(4)]; and

(5) the name, address, telephone number, and e-mail address of the employee or agent of the covered entity from whom additional information may be obtained about the breach.

The covered entity must provide the following information to the Department of Legal Affairs upon its request:

(1) a police report, incident report, or computer forensics report;

(2) a copy of the policies in place regarding breaches; and

(3) steps that have been taken to rectify the breach.

Under § 501.171(5), if consumer credit reporting agencies must be notified, the notice shall include the timing, distribution, and content of the notice provided to affected individuals.

Under § 501.171(6), third-party agents providing notice to covered entities must provide the covered entity with all information the covered entity needs to comply with its notice requirements.

ARE THERE ANY EXEMPTIONS?

Under § 501.171(4)(b), if a federal, state, or local law enforcement agency determines that notice to individuals required under this subsection would interfere with a criminal investigation, the notice shall be delayed upon the written request of the law enforcement agency for a specified period that the law enforcement agency determines is reasonably necessary. A law enforcement agency may, by a subsequent written request, revoke such delay as of a specified date or extend the period set forth in the original request made under this paragraph to a specified data if further delay is necessary.

Under § 501.171(4)(c), notice to the affected individuals is not required if, after an appropriate investigation and consultation with relevant federal, state, or local law enforcement agencies, the covered entity reasonably determines that the breach has not and will not likely result in identify theft or any other financial harm to the individuals whose personal information has been accessed. Such a determination must be documented in writing and maintained for at least 5 years. The covered entity shall provide the written determination to the Department of Legal Affairs within 30 days after the determination.

Under § 501.171(4)(g), notice provided pursuant to the rules, regulations, procedures, or guidelines established by the covered entity's primary or functional federal regulator is deemed to be in compliance with the notice requirements in this subsection if the covered entity notifies affected individuals in accordance with the rules, regulations, procedures, or guidelines established by the primary or functional federal regulator in the event of a breach of security. A covered entity that timely provides a copy of such notice to the Department of Legal Affairs is deemed to be in compliance with the notice requirements of § 501.171(3).

Under § 501.171(3)(e), if the covered entity is the judicial branch, the Executive Office of the Governor, the Department of Financial Services, or the Department of Agriculture and Consumer

Services, in lieu of providing the written notice to the Department of Legal Affairs, the covered entity may post all the information described in § 501.171(3)(b) on an agency-managed website.

WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

Under § 501.171(9)(a), the violations are treated as an unfair or deceptive trade practice and may be enforced by the Florida Department of Legal Affairs. In addition to the remedies provided for in paragraph (a), a covered entity that violates subsection (3) or subsection (4) shall be liable for a civil penalty not to exceed $500,000, as follows:

(1) In the amount of $1,000 for each day up to the first 30 days following any violation of subsection (3) or subsection (4) and, thereafter, $50,000 for each subsequent 30-day period or portion thereof for up to 180 days.

(2) If the violation continues for more than 180 days, in an amount not to exceed $500,000.

The civil penalties for failure to notify provided in this paragraph apply per breach and not per individual affected by the breach.

All penalties collected pursuant to this subsection shall be deposited into the General Revenue Fund.

ARE THERE ANY DATA SECURITY REQUIREMENTS IMPOSED?

Under § 501.171(2), each covered entity, governmental entity, or third-party agent shall take reasonable measures to protect and secure data in electronic form containing personal information.

Sections 282.0041 and 282.318 impose additional security requirements on entities.

ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

None.

GEORGIA

STATUTE: Ga. Code §§ **10-1-910, -911, -912;**[24] **§ 46-5-214**.[25]

WHO MUST COMPLY?

Under § 10-1-912(a), any information broker or data collector that maintains computerized data that includes personal information of individuals must comply.

Under § 10-1-912(b), any person or business that maintains computerized data on behalf of an information broker or data collector that includes personal information of individuals that the person or business does not own must comply.

Under § 10-1-911(2), "data collector" means any state or local agency or subdivision thereof including any department, bureau, authority, public university or college, academy, commission, or other government entity; provided, however, that the term "data collector" shall not include any governmental agency whose records are maintained primarily for traffic safety, law enforcement, or licensing purposes or for purposes of providing public access to court records or to real or personal property information.

Under § 10-1-911(3), "information broker" means any person or entity who, for monetary fees or dues, engages in whole or in part in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring, or communication information concerning individuals for the primary purpose of furnishing personal information to nonaffiliated third parties, but does not include any governmental agency whose records are maintained primarily for traffic safety, law enforcement, or licensing purposes.

Under § 10-1-911(5), "person" means any individual, partnership, corporation, limited liability company, trust, estate, cooperative, association or other entity. The term "person" as used in this article shall not be construed to require duplicative reporting by any individual, corporation, trust, estate, cooperative, association, or other entity involved in the same transaction.

WHAT DATA IS COVERED?

Under § 10-1-912(a) and (b), personal information is covered. Under § 10-1-911(6), "personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:

(1) social security number;

(2) driver's license number or state identification card number;

[24] Publicly available at: *Georgia General Assembly, Legislation*, www.legis.ga.gov, http://www.legis.ga.gov/Legislation/en-US/display/20072008/SB/236 (last visited June 12, 2019).
[25] Publicly available at: *elaws.us*, www.ga.ewlaws.us**,** http://ga.elaws.us/law/section46-5-214 (last visited June 12, 2019).

(3) account number, credit card number, or debit card number, if circumstances exist wherein such a number could be used without additional identifying information, access codes, or passwords;

(4) account passwords or personal identification numbers or other access codes; or

(5) any of the items contained in subparagraphs (1) through (4) of this paragraph when not in connection with the individual's name, if the information compromised would be sufficient to perform or attempt to perform identity theft against the person whose information was compromised.

The term "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

WHAT CONSTITUTES A DATA BREACH?

Under § 10-1-911(1), a data breach means unauthorized acquisition of an individual's electronic data that compromises the security, confidentiality, or integrity of personal information of such individual maintained by an information broker or data collector.

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

WHO MUST BE NOTIFIED?

Under § 10-1-912(a), any resident of Georgia or information broker or data collector whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person must be notified.

Under § 10-1-912(b), any person or business maintaining computerized data that includes personal information of individuals that the person or business does not own shall notify the broker or data collector if the person's information was, or is reasonably believed to have been, acquired by an unauthorized person.

Under § 10-1-912(d), if an information broker or data collector must notify more than 10,000 residents of Georgia at one time, the information broker or data collector shall also notify, all consumer reporting agencies that compile and maintain files on consumers on a nation-wide basis, as defined by 15 U.S.C. § 1681(a).

WHEN MUST NOTICE BE SENT?

Under § 10-1-912(a), notice shall be made in the most expedient time possible and 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, security, and confidentiality of the data system.

Under § 10-1-912(b), if a person or business that does not own personal information has to notify the information broker or data collector who does own the personal information, notice shall be made within 24 hours.

Under § 10-1-912(d), if an information broker or data collector has to notify consumer reporting agencies, they must notify the consumer reporting agencies without unreasonable delay.

IN WHAT FORM AND MANNER MUST NOTICE BE SENT?

Under § 10-1-911(4), notice may be provided by one of the following methods:

(1) written notice;

(2) telephone notice;

(3) electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in § 7001 of Title 15 of the United States Code; or

(4) substitute notice, if the information broker or data collector demonstrates that the cost of providing notice would exceed $50,000.00, that the affected class of individuals to be notified exceeds 100,000, or that the information broker or data collector does not have sufficient contact information to provide written or electronic notice to such individuals.

Substitute notice shall consist of all of the following:

(1) email notice, if the information broker or data collector has an e-mail address for the individuals to be notified;

(2) conspicuous posting of the notice on the information broker's or data collector's website page, if the information broker or data collector maintains one; and

(3) notification to major state-wide media.

WHAT MUST THE NOTICE SAY?

No specific requirements. The notice must simply carry out its purpose of notifying affected individuals of the breach.

Under § 10-1-912(d), if a consumer reporting agency must be notified, the notice must include the timing, distribution, and content of notices sent to affected individuals.

ARE THERE ANY EXEMPTIONS?

Under § 10-1-912, the notification may be delayed if a law enforcement agency determines that the notification will compromise a criminal investigation. The notification required shall be made after the law enforcement agency determines that it will not compromise the investigation.

Under § 10-1-911(4), if an information broker or data collector maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this article, they shall be deemed to be in compliance with the notification requirements of this article if it notifies the individuals who are the subjects of the notice in accordance with its policies in the event of a breach of the security system.

Under § 46-5-214, the notice required by this Code section shall be delayed if a law enforcement agency informs the business that notification may impede a criminal investigation or jeopardize national or homeland security.

WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

The statutes are unclear as to who may enforce and what penalties may be imposed. There is no express limitation of enforcement to only government entities, so private actions may be available. However, certain industry-specific statutes, such as the statute concerning telecommunications companies (discussed below) are explicitly enforceable by the Attorney General.

ARE THERE ANY DATA SECURITY REQUIREMENTS IMPOSED?

None.

ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

Insurance. *See* http://rules.sos.ga.gov/gac/120-2-87. The purpose of this regulation is to implement the provisions of Chapter 39 of Title 33 of the Official Code of Georgia Annotated and to provide an interpretive ruling to carry out the responsibilities of the Office of the Commissioner concerning the collection, use, and disclosure of personal information in connection with insurance transactions in Georgia pursuant to Title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 *et seq.*).

This regulation is issued pursuant to the authority vested in the Commissioner of Insurance under O.C.G.A. § 33-2-9 to implement Chapter 39 of Title 33 and to provide an interpretive ruling to carry out the responsibilities of his office under Sections 505 and 507 of Subtitle A of Title V of the Gramm-Leach-Bliley Act. Section 505 of the Gramm-Leach-Bliley Act specifically reserves functional regulation of all insurance activities to the States and directs State insurance authorities to enforce Title V privacy standards, and Section 507 permits the enforcement of any State provisions that offer greater protections and standards than may be set forth in Title V of the Gramm-Leach-Bliley Act.

The Commissioner of Insurance may enforce this statute.

Telecommunications. *See* http://ga.elaws.us/law/section46-5-214. In the event of a breach of a telephone record concerning a Georgia resident, the telecommunication company must provide notice to the Georgia resident immediately following discovery or notification of the breach if such breach is likely to cause quantifiable harm to the Georgia resident. The notice must be made in the most expedient manner possible and without unreasonable delay, consistent with any

measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the phone record.

Under § 46-5-214(b), if a telecommunications company maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this Code section, they shall be deemed to be in compliance with the notification requirements of this Code section if it notifies the individuals who are the subject of the notice in accordance with its policies in the event of a breach of the security of the system.

Under § 46-5-214(c), the notice shall be delayed if a law enforcement agency informs the business that notification may impede a criminal investigation or jeopardize national or homeland security, provided that such request is made in writing or the business documents such request contemporaneously in writing, including the name of the law enforcement officer making the request and the officer's law enforcement agency engaged in the investigation. The notice required by this section shall be provided without unreasonable delay after the law enforcement agency communicates to the business its determination that notice will no longer impede the investigation or jeopardize national or homeland security.

Under § 46-5-214(d), a violation of this Code section constitutes an unfair or deceptive practice in consumer transactions within the meaning of Part 2 of Article 15 of Chapter 1 of Title 10, the "Fair Business Practices Act of 1975." The Fair Business Act states that "[a]ny person who violates the terms of an injunction issued under Code **§** 10-1-397 shall forfeit and pay to the state a civil penalty of not more than $25,000.00 per violation." Ga. Code Ann. § 10-1-405.

GUAM

STATUTE: 9 GCA § **48-10** ***et seq.***[26]

WHO MUST COMPLY?

Under § 48.30(a), an individual or entity that owns or licenses computerized data that includes personal information must comply.

Under § 48.30(c), 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 believe was, accessed and acquired by an unauthorized person.

Under § 48.20(b), "entity" includes corporations, business trusts, estates, partnerships, limited partnerships, limited liability partnerships, limited liability companies, associations, organizations, joint ventures, governments, governmental subdivisions, agencies, or instrumentalities, or any other legal entity, whether for profit or not-for-profit.

Under § 48.20(e), "individual" means a natural person.

WHAT DATA IS COVERED?

Under § 48.30(a), unencrypted and unredacted personal information is covered.

Under § 48.20(f), "personal information" means the first name, or first initial, and last name in combination with and linked to any one or more of the following data elements that relate to a resident of Guam, when the data elements are neither encrypted nor redacted:

(1) Social Security number;

(2) driver's license number or Guam identification card number issued in lieu of a driver's license; or

(3) financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial accounts.

The term does not include information that is lawfully obtained from publicly available information, or from Federal, State, or local government records lawfully made available to the general public.

Under § 48.20(c), "encrypted" means transformation of data through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without the use of a confidential process or key, or securing the information by another method that renders the data elements unreadable or unusable.

[26] Publicly available at: *Title 9 Criminal and Correction Code*, www.guamcourts.org, http://www.guamcourts.org/compileroflaws/GCA/09gca/9gc048.pdf (last visited June 12, 2019).

WHAT CONSTITUTES A DATA BREACH?

Under § 48.20(a), data breach means the unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes, or the individual or entity reasonably believes has caused or will cause, identity theft or other fraud to any resident of Guam.

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

Under § 48.30(b), an individual or entity must disclose the breach of the security of the system if the encrypted information is accessed and acquired in an unencrypted form, or if 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.

WHO MUST BE NOTIFIED?

Under § 48.30(a), any resident of Guam whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person and that causes, or the individual or entity reasonably believes has caused or will cause, identity theft or fraud to any resident of Guam must be notified.

WHEN MUST NOTICE BE SENT?

Under § 48.30(a), the disclosure shall be made without unreasonable delay.

Under § 48.30(c), disclosure to an owner or licensee of a breach of information must be made as soon as practicable following discovery.

IN WHAT FORM AND MANNER MUST NOTICE BE SENT?

Under § 48.20(g), notice may be provided by one of the following methods:

(1) written notice to the postal address in the records of the individual or entity;

(2) telephone notice;

(3) electronic notice; or

(4) substitute notice, if the individual or the entity required to provide notice demonstrates that the cost of providing notice will exceed $10,000, or that the affected class of residents to be notified exceeds 5,000 persons, or that the individual or the entity does not have sufficient contact information or consent to provide notice as described in paragraphs 1, 2, or 3.

Substitute notice consists of any two of the following:

(1) email notice if the individual or the entity has email addresses for the members of the affected class of residents;

(2) conspicuous posting of the notice on the Website of the individual or the entity, if the individual or the commercial entity maintains a Website; and

(3) notice to major Guam media.

WHAT MUST THE NOTICE SAY?

No specific requirements. The notice must simply carry out its purpose of notifying affected individuals of the breach.

ARE THERE ANY EXEMPTIONS?

Under § 48.30(d), notice required by this section 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. Notice required by this section must be made without unreasonable delay after the law enforcement agency determines that notification will no longer impede the investigation or jeopardize national or homeland security.

Under § 48.30(a), disclosure shall be made without unreasonable delay except in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the system.

Under § 48.40(a), any entity that maintains its own notification procedures as part of an information privacy or security policy for the treatment of personal information and that are consistent with the timing requirements of this Chapter shall be deemed to be in compliance with the notification requirements of this chapter if it notifies residents of Guam in accordance with its procedures in the event of a breach of security of the system.

Under § 48.50(b)(2), an entity that complies with the notification requirements or procedures pursuant to the rules, regulations, procedures, or guidelines established by the entity's primary or functional Federal regulator shall be in compliance with this Chapter.

WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

Under § 48.50(a), a violation of this chapter that results in injury or loss to residents of Guam may be enforced by the Office of the Attorney General. Except as provided by § 48.40 of this Chapter, the Office of the Attorney General shall have 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.

ARE THERE ANY DATA SECURITY REQUIREMENTS IMPOSED?

Section § 48.10 states that "both public and private entities on Guam have a duty to safeguard personal information that, if stolen or publicized, may result in crimes such as fraud and identity theft…[I]t is incumbent upon all entities that are entrusted with such data to maintain strong security systems to ensure that all personal information will always be protected." But there are no explicit system requirements set forth in the statute.

ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

Under § 48.40(b)(1), a financial institution that complies with the notification requirements prescribed by the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice is deemed to be in compliance with this Chapter.

Under § 48.20(d), financial institution means any institution the business of which is engaging in financial activities as described in 12 U.S.C. 1843(k).

HAWAII

STATUTE: Haw. Rev. Stat. § 487N-1 *et seq.*[27]

WHO MUST COMPLY?

Under § 487N-2(a), any business that owns or licenses personal information of residents of Hawaii, any business that conducts business in Hawaii that owns or licenses personal information in any form (whether computerized, paper, or otherwise), or any government agency that collects personal information for specific government purposes must comply.

Under § 487N-2(b), any business located in Hawaii or any business that conducts business in Hawaii that maintains or possesses records or data containing personal information of residents of Hawaii that the business does not own or license, or any government agency that maintains or possesses records or data containing personal information of residents of Hawaii shall comply.

Under § 487N-1, "business" means a sole proprietorship, partnership, corporation, association, or other group, however organized, and whether or not organized to operate at a profit. The term includes a financial institution organized, chartered, or holding a license or authorization certificate under the laws of the State, any other state, the United States, or any other country, or the parent or the subsidiary of any such financial institution. The term also includes an entity whose business is records destruction.

Under § 487N-1, "government agency" means the department, division, board, commission, public corporation, or other agency or instrumentality of the State or of any county.

WHAT DATA IS COVERED?

Under § 487N-2(a) and (b), personal information is covered. Under § 487N-1, "personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(1) social security number;

(2) driver's license number or Hawaii identification card number; or

(3) account number, credit or debit card number, access code, or password that would permit access to an individual's financial account.

"Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

[27] Publicly available at: *Hawaii State Legislature*, www.capitol.hawaii.gov, http://www.capitol.hawaii.gov/hrs.aspx?query=487N-1 (last visited June 12, 2019).

WHAT CONSTITUTES A DATA BREACH?

Under § 487N-1, data breach means an incident of unauthorized access to and acquisition of unencrypted or unredacted records or data containing personal information where illegal use of the personal information has occurred, or is reasonably likely to occur and that creates a risk of harm to a person. Any incident of unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential process or key constitutes a breach.

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

WHO MUST BE NOTIFIED?

Under § 487N-2, any affected persons and the owner or licensee of the information involved in any security breach must be notified.

Under § 487N-2(f), in the event a business provides notice to more than 1,000 persons at a time pursuant to this section, the business shall notify the State of Hawaii's office of consumer protection and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. § 1681a(p).

WHEN MUST NOTICE BE SENT?

Under § 487N-2(a), notice shall be made without unreasonable delay, consistent with the legitimate needs of law enforcement as provided in subsection (c) of this section, 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.

Under § 487N-2(b), notice to the owner or licensee of information shall be made immediately following discovery of the breach, consistent with the legitimate needs of law enforcement as provided in subsection (c) of this section.

Under § 487N-2(c), notice to the State of Hawaii's office of consumer protection and all consumer reporting agencies shall be made without unreasonable delay.

IN WHAT FORM AND MANNER MUST NOTICE BE SENT?

Under § 487N-2(e), notice to affected persons may be provided by one of the following methods:

(1) written notice to the last available address the business or government agency has on record;

(2) electronic mail notice, for those persons for whom a business or government agency has a valid electronic mail address and who have agreed to receive communications electronically if the notice provided is consistent with the

provisions regarding electronic records and signatures for notices legally required to be in writing set forth in 15 U.S.C. § 7001;

(3) telephonic notice, provided that contact is made directly with the affected persons; and

(4) substitute notice, if the business or government agency demonstrates that the cost of providing notice would exceed $100,000 or that the affected class of subject persons to be notified exceeds 200,00, or if the business or government agency does not have sufficient contact information or consent to satisfy paragraph (1), (2), or (3), for only those affected persons without sufficient contact information or consent, or if the business or government agency is unable to identify particular affected persons, for only those unidentifiable affected persons.

Substitute notice shall consist of all of the following:

(1) electronic mail notice when the business or government agency has an electronic mail address for the subject persons;

(2) conspicuous posting of the notice on the website page of the business or government agency, if one is maintained; and

(3) notification to major statewide media.

Under § 487N-2(f), notice to the State of Hawaii's office of consumer protection and all consumer reporting agencies shall be in writing.

WHAT MUST THE NOTICE SAY?

Under § 487N-2(d), the notice should include a description of the following:

(1) the incident in general terms;

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

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

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

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

Under § 487N-2(f), notice to the State of Hawaii's office of consumer protection and all consumer reporting agencies shall include the timing, distribution, and content of the notice made to affected individuals.

ARE THERE ANY EXEMPTIONS?

Under § 487N-2(c), the notice required by this section shall be delayed if a law enforcement agency informs the business or government agency that notification may impede a criminal investigation or jeopardize national security and requests a delay; provided that such request is made in writing, or the business or government agency documents the request contemporaneously in writing, including the name of the law enforcement officer making the request and the officer's law enforcement agency engaged in the investigation. The notice required by this section shall be provided without unreasonable delay after the law enforcement agency communicated to the business or government agency and its determination that notice will no longer impede the investigation or jeopardize national security.

Under § 487N-2(g), the following businesses shall be deemed to be in compliance with this section:

(1) A financial institution that is subject to the federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice published in the Federal Register on March 29, 2005, by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision, or subject to 12 C.F.R. Part 748, and any revisions, additions, or substitutions relating to the interagency guidance; and

(2) Any health plan or healthcare provider that is subject to and in compliance with the standards for privacy or individually identifiable health information and the security standards for the protection of electronic health of the Health Insurance Portability and Accountability Act of 1996.

WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

Under § 487N-3(a), any business that violates any provision of this chapter shall be subject to penalties of not more than $2,500 for each violation. The Attorney General or the Executive Director of the Office of Consumer Protection may bring an action pursuant to this section. No such action may be brought against a government agency.

In addition to any penalty provided for in subsection (a), 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.

ARE THERE ANY DATA SECURITY REQUIREMENTS IMPOSED?

None.

Back to TOC

ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

None.

IDAHO

STATUTE: Idaho Code § 28-51-104 – 07.[28]

WHO MUST COMPLY?

Under § 28-51-105(1), a city, county or state agency, individual or commercial entity that conducts business in Idaho and that owns or licenses computerized data that includes personal information about a resident of Idaho must comply.

Under § 28-51-105(2), an agency, individual or commercial entity that maintains computerized data that includes personal information that the agency, individual or the commercial entity does not own or license must comply.

Under § 28-51-104(3), "commercial entity" includes corporation, business trust, estate, trust, partnership, limited partnership, limited liability partnership, limited liability company, association, organization, joint venture and any other legal entity, whether for profit or not-for-profit.

Under § 28-51-104(1), agency means any public agency, which is defined as any state agency or local agency. State agency means every state officer, department, division, bureau, commission and board or any committee of a state agency including those in the legislative or judicial branch, except the state militia and the Idaho state historical society library and archives. A local agency means a county, city, school district, municipal corporation, district, public health district, political subdivision, or any agency thereof, or any committee of a local agency, or any combination thereof.

WHAT DATA IS COVERED?

Under § 28-51-105, personal information is covered. Under §28-51-104(5), "personal information" means an Idaho resident's first name or first initial and last name in combination with any one or more of the following data elements that relate to the resident, when either the name or the data elements are not encrypted:

(1) social security number;

(2) driver's license number or Idaho identification card number; or

(3) account number, or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial account.

"Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.

[28] Publicly available at: *Idaho Statues*, www.legislature.idaho.gov, https://legislature.idaho.gov/statutesrules/idstat/Title28/T28CH51/SECT28-51-104/ (last visited June 12, 2019).

WHAT CONSTITUTES A DATA BREACH?

Under § 28-51-104, data breach means the illegal acquisition of unencrypted computerized data that materially compromises the security, confidentiality, or integrity of personal information for 1 or more persons maintained by an agency, individual or a commercial entity.

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

WHO MUST BE NOTIFIED?

Under § 28-51-105(1), an affected Idaho resident must be notified if it is determined that the misuse of information about that resident has occurred or is reasonably likely to occur.

Under § 28-51-105(2), an agency, individual or commercial entity that maintains computerized data that includes personal information that the agency, individual or commercial entity does not own or license shall give notice to the owner or licensee of the information of any breach if misuse of personal information about an Idaho resident occurred or is reasonably likely to occur.

Under § 28-51-105(1), when an agency becomes aware of a breach of the security of the system, it shall notify the office of the Idaho Attorney General. This 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 Idaho technology authority policies.

WHEN MUST NOTICE BE SENT?

Under § 28-51-105(2), notice to the owner or licensee of the information of the breach must be given immediately following discovery of a breach.

Under § 28-51-105(1), notice to the Idaho Attorney General must be given within 24 hours of discovery.

IN WHAT FORM AND MANNER MUST NOTICE BE SENT?

Under § 28-51-104(4), notice may be sent in any of the following manners:

(1) written notice to the most recent address the agency, individual or commercial entity has in its records;

(2) telephonic notice;

(3) electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. **§** 7001; or

(4) substitute notice, if the agency, individual or the commercial entity required to provide notice demonstrates that the cost of providing notice will exceed $25,000,

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

Substitute notice consists of all of the following:

(1) email notice if the agency, individual or the commercial entity has email addresses for the affected Idaho residents;

(2) conspicuous posting of the notice on the website page of the agency, individual or the commercial entity if the agency, individual or the commercial entity maintains one; and

(3) notice to major statewide media.

WHAT MUST THE NOTICE SAY?

No specific requirements. The notice must simply carry out its purpose of notifying affected individuals of the breach.

ARE THERE ANY EXEMPTIONS?

Under § 28-51-105(3), notice required may be delayed if a law enforcement agency advises the agency, individual or commercial entity that the notice will impede a criminal investigation. Notice required by this section must be made in good faith, without unreasonable delay, and as soon as possible after the law enforcement agency advises the agency, individual, or commercial entity that notification will no longer impede the investigation.

Under § 28-51-106(1), an agency, individual, or a commercial entity that maintains its own notice procedures as part of an information security policy for the treatment of personal information, and whose procedures are otherwise consistent with the timing requirements of § 28-51-105, is deemed to be in compliance with the notice requirement of § 28-51-105, if the agency, individual, or the commercial entity notifies affected Idaho residents in accordance with its policies in the event of a breach of security of the system.

Under § 28-51-106(2), an individual or commercial entity that is regulated by state or federal law and that maintains procedures for a breach of the security of the system pursuant to the laws, rules, regulations, guidances, or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance with § 28-51-105, if the individual or the commercial entity complies with the maintained procedures when a breach of the security of the system occurs.

WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

Under § 28-51-107, in any case in which an agency's, commercial entity's or individual's primary regulator has reason to believe that an agency, individual or commercial entity subject to that primary regulator's jurisdiction under **§** 28-51-104(6) has violated **§** 28-51-105 by failing to give notice in accordance with that section, the primary regulator may bring a civil action to

enforce compliance with that section and enjoin that agency, individual or commercial entity from further violations. Any agency, individual or commercial entity that intentionally fails to give notice in accordance with § 28-51-105 shall be subject to a fine of not more than $25,000 per breach of the security of the system.

ARE THERE ANY DATA SECURITY REQUIREMENTS IMPOSED?

None.

ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

None.

ILLINOIS

STATUTE: 815 Ill. Comp. Stat. § 530/1-530/50.[29]

WHO MUST COMPLY?

Under 815 Ill. Comp. Stat. § 530/10(a), any data collector that owns or licenses personal information concerning an Illinois resident must comply. "Data collector" may include, but is not limited to, government agencies, public and private universities, privately and publicly held corporations, financial institutions, retail operators, and any other entity that, for any purpose, handles, collects, disseminates, or otherwise deals with nonpublic personal information.

Under 815 Ill. Comp. Stat. § 530/10(b), any data collector that maintains or stores, but does not own or license, computerized data that includes personal information that the data collector does not own or license shall comply if personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Under 815 Ill. Comp. Stat. § 530/12, any State Agency that collects personal information concerning an Illinois resident must comply.

WHAT DATA IS COVERED?

Personal information is covered. Under 815 Ill. Comp. Stat. § 530/5, "personal information" means either of the following:

(1) an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the name or data elements have been acquired without authorization through the breach of security:

(1) social security number.

(2) driver's license number or State identification card number.

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

(4) Medical information meaning any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional, including such information provided to a website or a mobile application.

[29] Publicly available at: *Illinois Compiled Statues*, www.ilga.gov, http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=2702&ChapAct=815 ILCS 530/&ChapterID=67&ChapterName=BUSINESS+TRANSACTIONS&ActName=Personal+Information+Protection+Act (last visited June 12, 2019).

(5) Health insurance information meaning an individual's health insurance policy number or subscriber identification number, any unique identifier, used by a health insurer to identify the individual, or any medical information in an individual's health insurance application and claims history, including any appeals records.

(6) Unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee to authenticate an individual, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data.

(2) user name or email address, in combination with any password or security question and answer that would permit access to an online account, when either the user name or email address and password or security question and answer are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the data elements have been obtained through the breach of security.

"Personal information" does not include publicly available information that is lawfully made available to the general public from federal, State, or local government records.

WHAT CONSTITUTES A DATA BREACH?

Under 815 Ill. Comp. Stat. § 530/5, a data breach means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the data collector.

Data breach does not include good faith acquisition of personal information by an employee or agent of the data collector for a legitimate purpose of the data collector, provided that the personal information is not used for a purpose unrelated to the data collector's business or subject to further unauthorized disclosure.

WHO MUST BE NOTIFIED?

Any affected Illinois resident or the owner or licensee of the information must be notified.

Under 815 Ill. Comp. Stat. § 530/12(d), if a State Agency is required to notify more than 1,000 persons of a breach of security, the State Agency shall also notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by 15 U.S.C. § 1681a(p).

If a State Agency suffers a single breach of the security of the data concerning personal information of more than 250 Illinois residents, they shall notify the Attorney General of the breach. In this circumstance, if the State agency is directly responsible to the Governor, and they have been subject to or have reason to believe they have been subject to a breach of security concerning more than 250 Illinois residents or that there was an instance of aggravated computer

tampering, they shall notify the Office of the Chief Information Security Officer of the Illinois Department of Innovation and Technology and the Attorney General regarding the breach or instance of aggravated computer tampering.

If a State Agency determines the identity of the actor who perpetrated the breach, then the agency shall report this information, within 5 days after the determination, to the General Assembly, provided that such report would not jeopardize the security of Illinois residents or compromise a security investigation.

WHEN MUST NOTICE BE SENT?

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

If any data collector that maintains or stores, but does not own or license, computerized data has to notify the owner or licensee of the information of a breach, they must notify the owner or licensee immediately following discovery.

Under 815 Ill. Comp. Stat. § 530/12, notice by State Agencies must be provided in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.

If a State Agency must notify all consumer reporting agencies, they must do so without unreasonable delay.

If a State Agency has to notify the Attorney General, it must be made within 45 days of the State agency's discovery of the security breach or when the State agency provides any notice to consumers required by this section, whichever is sooner, unless the State agency has good cause for reasonable delay to determine the scope of the breach and restore the integrity, security, and confidentiality of the data system, or when law enforcement requests in writing to withhold disclosure of some or all of the information required in the notification under this Section.

Notice to the Office of the Chief Information Security Officer of the Illinois Department of Innovation and Technology must be made without delay, but no later than 72 hours following the discovery of the incident.

IN WHAT FORM AND MANNER MUST NOTICE BE SENT?

Under 815. Ill. Comp. Stat. § 530/10(c), notice to residents may be provided by one of the following methods:

(1) written notice;

(2) electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures for notices legally required to be in writing as set forth in § 7001 of Title 15 of the United States Code; or

(3) substitute notice, if the data collector demonstrates that the cost of providing notice would exceed $250,000 or that the affected class of subject persons to be notified exceeds 500,000, or the data collector does not have sufficient contact information.

Substitute notice shall consist of all of the following:

(1) email notice if the data collector has an email address for the subject persons;

(2) conspicuous posting of the notice on the data collector's web site page if the data collector maintains one; and

(3) notification to major statewide media or, if the breach impacts residents in one geographic area, to prominent local media in areas where affected individuals are likely to reside if such notice is reasonably calculated to give actual notice to persons whom notice is required.

WHAT MUST THE NOTICE SAY?

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

If the breached personal information includes user names or email addresses, in combination with a password or security question and answer that would permit access to an online account, notice must direct the Illinois resident whose personal information has been breached to promptly change his or her user name or password and security question or answer, as applicable, or to take other steps appropriate to protect all online accounts for which the resident uses the same user name or email address and password or security question and answer.

If a State Agency must notify all consumer reporting agencies, they must notify them of the timing, distribution, and content of the notices sent to affected residents.

Notice to the Attorney General must include the types of personal information compromised in the breach, the number of Illinois residents affected by such incident at the time of notification, any steps the State agency has taken or plans to take relating to notification of the breach to consumers, and the date and timeframe of the breach, if known at the time notification is provided.

ARE THERE ANY EXEMPTIONS?

The notification to an Illinois resident required by subsection (a) of the statute may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the data collector with a written request for the delay. The data

collector must notify the Illinois resident as soon as notification will no longer interfere with the investigation.

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

WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

A violation of this Act constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act, which may be enforced by the Attorney General. 815 Ill. Comp. Stat. 530/20. If an individual can show actual damages, he or she may be able to sue for a violation of the Act in federal court. *See Dieffenbach v. Barnes & Noble, Inc.*, 887 F.3d 826, 830 (7th Cir. 2018) (finding that a consumer paying money for credit monitoring services to be a form of "actual damage" sufficient for standing).

ARE THERE ANY DATA SECURITY REQUIREMENTS IMPOSED?

Under 815 Ill. Comp. Stat. 530/45(a), a data collector that owns or licenses, or maintains or stores but does not own or license, records that contain personal information concerning an Illinois resident shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure.

Under 815 Ill. Comp. Stat. 530/45(b), a contract for the disclosure of personal information concerning an Illinois resident that is maintained by a data collector must include a provision requiring the person to whom the information is disclosed to implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure.

Under 815 Ill. Comp. Stat. 530/45(c), if a state or federal law requires a data collector to provide greater protection to records that contain personal information concerning an Illinois resident that are maintained by the data collector and the data collector is in compliance with the provisions of that state or federal law, the data collector shall be deemed to be in compliance with the provisions of this Section.

ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

Under 815 Ill. Comp. Stat. 530/45, a data collector that owns or licenses, or maintains or stores but does not own or license, records that contain personal information concerning an Illinois resident is required to implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure.

Under 815 Ill. Comp. Stat. 53/50, entities subject to the Federal Health Insurance Portability and Accountability Act of 1996 are required to provide notification of a breach to the Secretary of Health and Human Services pursuant to the Health Information Technology for Economic and

Clinical Health Act and also provide notification to the Attorney General within five business days of notifying the Secretary.

INDIANA

STATUTE: Ind. Code §§ 4-1-11 *et seq.*, 24-4.9 *et seq.*[30]

WHO MUST COMPLY?

Any person or state agency that owns or licenses computerized data that includes personal information must comply.

"State agency" means an authority, a board, a branch, a commission, a committee, a department, a division, or another instrumentality of the executive, including the administrative, department of state government. Except as provided in (4), the term does not include the judicial or legislative department of state government. The term includes the following: (1) a state elected official's office, (2) a state educational institution, (3) a body corporate and politic of the state created by state statute, and (4) the Indiana lobby registration commission established by IC 2-7-1.6-1.

"Person" means an individual, a corporation, a business trust, an estate, a trust, a partnership, an association, a nonprofit corporation or organization, a cooperative, or any other legal entity.

Any person or state agency that maintains computerized data but that is not a data base owner must comply to the extent they must notify the data base owner if they discover that personal information was or may have been acquired by an unauthorized person.

WHAT DATA IS COVERED?

"Personal information," meaning:

Under § 4-1-11-3, applicable to State Agencies, information consisting of an individual's first name and last name or first initial and last name and at least one of the following:

(1) social Security number;

(2) driver's license number or identification card number; or

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

The term does not include the following:

(1) the last four (4) digits of an individual's social security number; or

(2) publicly available information that is lawfully made available to the public from records of a federal agency or local agency.

[30] Publicly available at: *2017 Archived Indiana Code*, www.iga.in.gov, https://iga.in.gov/legislative/laws/2017/ic/titles/024 (last visited June 12, 2019)

Under § 24-4.9-2-10, applicable to Persons or a Business, a social security number that is not encrypted or redacted; or unencrypted or unredacted information consisting of an individual's first and last names and one or more of the following:

(1) driver's license number;

(2) state identification card number;

(3) credit card number; or

(4) financial account number or debit card number in combination with a security code, password, or access code that would permit access to the person's account.

The term "personal information" does not include information that is lawfully obtained from publicly available information or from federal, state, or local government records lawfully made available to the general public.

WHAT CONSTITUTES A DATA BREACH?

A data breach means the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person or a state or local agency.

The term does not include the following:

(1) the good faith acquisition of personal information by an agency or employee of the person or agency for purposes of the person or agency, if the personal information is not used or subject to further unauthorized disclosure; or

(2) the unauthorized acquisition of a portable electronic device on which personal information is stored if access to the device is protected by a password that has not been disclosed, or in the case of a person or business, is protected by encryption and the encryption key that has not been compromised or disclosed or is not in the possession of or known to the person who, without authorization, acquired or has access to the portable electronic device.

WHO MUST BE NOTIFIED?

Any state resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person, or whose encrypted personal information was or may have been acquired by an unauthorized person with access to the encryption key, if the data base owner knows, should know, or should have known that the unauthorized acquisition constituting the breach has resulted in or could result in identity deception (as defined in IC 35-43-5-3.5), identity theft, or fraud affecting the Indiana resident, must be notified.

If disclosure to more than 1,000 consumers is required, then all consumer reporting agencies shall also be notified of all information necessary to assist the consumer reporting agency in

preventing fraud, including personal information of an Indiana resident affected by the breach of the security of a system.

If a data base owner make a disclosure, they shall also disclose the breach to the Attorney General.

WHEN MUST NOTICE BE SENT?

Notice must be sent without unreasonable delay. A delay is reasonable if it is necessary to restore the integrity of the computer systems; it is necessary to discover the scope of the breach; or it is in response to a request from the attorney general or a law enforcement agency to delay disclosure because disclosure will impede a criminal or civil investigation; or jeopardize national security.

A person required to make disclosure or notification shall make disclosure or notification as soon as possible after delay is no longer necessary to restore the integrity of the computer system or to discover the scope of the breach; or the attorney general or law enforcement agency notifies the person that delay will no longer impede a criminal or civil investigation or jeopardize national security.

IN WHAT FORM AND MANNER MUST NOTICE BE SENT?

Except as provided in section 9 of this chapter, a state agency may provide the notice required under this chapter (a):

(1) in writing; or

(2) by electronic mail, if the individual has provided the state agency with the individual's electronic mail address.

This section applies if a state agency demonstrates that:

(1) the cost of providing the notice required under this chapter is at least $250,000;

(2) the number of persons to be notified is at least 500,000; or

(3) the agency does not have sufficient contact information; the state agency may use an alternate form of notice.

A state agency may provide the following alternate forms of notice if authorized by subsection (a):

(1) conspicuous posting of the notice on the state agency's web site if the state agency maintains a web site; and

(2) notification to major statewide media.

A data base owner shall make disclosure using one of the following methods: (1) mail; (2) telephone; (3) facsimile; or (4) electronic mail, if the date base owner has the electronic mail address of the affected Indiana resident.

If a state agency can demonstrate that: (1) the cost of providing the notice required under this chapter is at least two hundred fifty thousand dollars $250,000; (2) the number of persons to be notified is at least 500,000, it can provide notice by using both of the following methods: (a) conspicuously posting of the notice on the web site of the data base owner, if the data base owner maintains a web site; and (b) providing notice to major news reporting media in the geographic area where Indiana residents affected by the breach of the security of a system reside.

If a database owner required to make disclosure under this chapter is required to make the disclosure to more than 500,000 Indiana residents, or if the data base owner required to make a disclosure under this chapter determines that the cost of the disclosure will be more than $250,000, the data base owner required to make a disclosure under this chapter may elect to make the disclosure by using both of the following methods: (1) conspicuous posting of the notice on the web site of the data base owner, if the data base owner maintains a website, and (2) notice to major news reporting media in the geographic area where Indiana residents affected by the breach of the security of a system reside.

WHAT MUST THE NOTICE SAY?

No specific requirements. The notice must simply carry out its purpose of notifying affected individuals of the breach.

ARE THERE ANY EXEMPTIONS?

The notification required by this chapter: (1) may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation; and (2) shall be made after the law enforcement agency determines that it will not compromise the investigation.

Under § 24-4.9-3-3.5; data base owners that maintain their own data security procedures as part of an information privacy, security policy, or compliance plan under the federal USA PATRIOT Act (P.L. 107-56), Executive Order 13224, the federal Driver's Privacy Protection Act (18 U.S.C. § 2721 et seq.), the Federal Fair Credit Reporting Act (15 U.S.C. § 1681 et seq.), the federal Financial Modernization Act of 1999 (15 U.S.C. 6801 et seq.) or the federal Health Insurance Portability and Accountability Act (HIPAA) (P.L. 104-191); and who do comply with the information privacy, security, privacy or compliance plan are exempt.

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

Back to TOC

WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

The Attorney General may bring an action to obtain any or all of the following: (1) an injunction to enjoin future violations; (2) a civil penalty of not more than $5,000 per deceptive act; and (3) the Attorney General's reasonable costs in the investigation of the deceptive act and maintaining the action.

ARE THERE ANY DATA SECURITY REQUIREMENTS IMPOSED?

Under IC 24-4.9-3-3.5(b), a data base owner shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect and safeguard from unlawful use or disclosure any personal information of Indiana residents collected or maintained by the data base owner.

ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

None.

IOWA

STATUTE: Iowa Code §§ 715C.1,[31] 715C.2,[32] **533.331**,[33] **279.71**[34]

WHO MUST COMPLY?

Under § 715C.2, 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 and that was subject to a breach of security must comply.

Under § 715C.2, any person who maintains or otherwise possesses personal information on behalf of another person shall comply.

"Person" means any individual; corporation; business trust; estate trust; partnership; limited liability company; association; joint venture; government; governmental subdivision, agency, or instrumentality; public corporation; or any other legal or commercial entity.

WHAT DATA IS COVERED?

Under § 715C.2, personal information is covered. "Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements that relate to the individual if any of the data elements are not encrypted, redacted, or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable or are encrypted, redacted, or otherwise altered by any method or technology but the keys to unencrypt, underact, or otherwise read the data elements have been obtained through the breach of security:

(1) social security number;

(2) driver's license number or other unique identification number created or collected by a government body;

(3) financial account number, credit card number, or debit card number in combination with any required expiration date, security code, access code, or password that would permit access to an individual's financial account;

(4) unique electronic identifier or routing code, in combination with any required security code, access code, or password that would permit access to an individual's financial account; or

[31] Publicly available at: *Chapter 715C Personal Information Security Breach Protection*, www.legis.iowa.gov, https://www.legis.iowa.gov/docs/code/715c.pdf (last visited June 12, 2019).
[32] *Id.*
[33] Publicly available at: *Data Breach – duty to notify*, www.legis.iowa.gov, https://www.legis.iowa.gov/docs/code/533.331.pdf (last visited June 12, 2019).
[34] Publicly available at: *Student online personal information protection*, www.legis.iowa.gov, https://www.legis.iowa.gov/docs/code/279.71.pdf (last visited June 11, 2019)

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

"Personal information" does not include information that is lawfully obtained from publicly available sources, or from federal, state, or local government records lawfully made available to the general public.

WHAT CONSTITUTES A DATA BREACH?

Under § 715C.1, a data breach means unauthorized acquisition of personal information maintained in computerized form by a person that compromises the security, confidentiality, or integrity of the personal information. It also means unauthorized acquisition of personal information maintained by a person in any medium, including on paper, that was transferred by the person to that medium from computerized form and that compromises the security, confidentiality; or integrity of the personal information.

Good faith acquisition of personal information by a person or that person's employee or agent for a legitimate purpose of that person is not a breach of security, provided that the personal information is not used in violation of applicable law or in a manner that harms or poses an actual threat to the security, confidentiality, or integrity of the personal information.

WHO MUST BE NOTIFIED?

Under § 715C.2, any consumer whose personal information was included in the information that was breached must be notified.

"Consumer" means an individual who is a resident of Iowa.

Any person who maintains or otherwise possesses personal information on behalf of another person must notify the owner or licensor of that information of any breach of security.

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 and that was subject to a breach of security requiring notification to more than 500 residents of this state pursuant to this section shall give written notice of the breach of security to the director of the consumer protection division of the attorney general.

WHEN MUST NOTICE BE SENT?

The consumer notification shall be made in the most expeditious manner possible and without unreasonable delay, consistent with the legitimate needs of law enforcement as provided in subsection 3, 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.

Notification to the owner or licensor of the information shall be made immediately following discovery of a breach if a consumer's personal information was included in the information that was breached.

Notice to the director of the consumer protection division of the office of the attorney general shall be made within 5 business days after giving notice of the breach to any consumer.

IN WHAT FORM AND MANNER MUST NOTICE BE SENT?

Notification to the consumer may be provided by one of the following methods:

(1) written notice to the last available address the person has in the person's records;

(2) electronic notice if the person's customary method of communication with the consumer is by electronic means or is consistent with the provisions regarding electronic records and signatures set forth in chapter 554D and the federal Electronic Signatures in Global and National Commerce Act, 15 U.S.C. § 7001; or

(3) substitute notice, if the person demonstrates that the cost of providing notice would exceed $250,000, that the affected class of consumers to be notified exceeds 350,000 persons, or if the person does not have sufficient contact information to provide notice.

Substitute notice shall consist of the following:

(1) electronic mail notice when the person has an electronic mail address for the affected consumers;

(2) conspicuous posting of the notice or a link to the notice on the Internet site of the person if the person maintains an internet website; and

(3) notification to major statewide media.

WHAT MUST THE NOTICE SAY?

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

(1) a description of the breach of security;

(2) the approximate date of the breach of security;

(3) the type of personal information obtained as a result of the breach of security;

(4) contact information for consumer reporting agencies; and

(5) advice to the consumer to report suspected incidents of identity theft to local law enforcement or the attorney general.

ARE THERE ANY EXEMPTIONS?

Notwithstanding subsection 1, notification is not required if, after an appropriate investigation or after consultation with the relevant federal, state, or local agencies responsible for law

enforcement, the person determined that no reasonable likelihood of financial harm to the consumers whose personal information has been acquired has resulted or will result from the breach. Such a determination must be documented in writing and the documentation must be maintained for 5 years.

The consumer notification requirement of this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation and the agency has made a written request that the notification be delayed. The notification required by this section shall be made after the law enforcement agency determines that the notification will not compromise the investigation and notifies the person required to give notice in writing.

Under § 715C.2(7), the notification requirements do not apply to any of the following:

(a) A person who complies with notification requirements or breach of security procedure that provide greater protection to personal information and at least as thorough disclosure requirements than that provided by this section pursuant to the rules, regulations, procedures, guidance, or guidelines established by the person's primary or functional federal regulator.

(b) A person who complies with a state or federal law that provides a greater protection to personal information and at least as thorough disclosure requirements for breach of security or personal information than that provided by this section.

(c) A person who is subject to and complies with regulations promulgated pursuant to Tit. V of the federal Gramm-Leach-Bliley Act of 1999, 15 U.S.C. §§ 6801–6809.

(d) A person who is subject to and complies with regulations promulgated pursuant to Tit. II, subtit. F of the federal Health Insurance Portability and Accountability Act of 1996 (HIPPA), 42 U.S.C. § 1320d – 1320d-9, and Tit. XIII, subtit. D of the federal Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH), 42 U.S.C. §§ 17921–17954.

WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

A violation of this chapter is an unlawful practice pursuant to § 714.16 and, in addition to the remedies provided to the Attorney General pursuant to § 714.16(7), the Attorney General may seek and obtain an order that a party held to violate this section pay damages to the Attorney General on behalf of a person injured by the violation.

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

Under § 714.16(7), the Attorney General may seek and obtain in an action in a district court a temporary restraining order, preliminary injunction, or permanent injunction prohibiting the person from continuing the practice or engaging in the practice or doing an act in furtherance of the practice. The court may make orders or judgments as necessary to prevent the use or employment by a person of any prohibited practices, or which are necessary to restore to any

person in interest any moneys or property, real or personal, which have been acquired by means of a practice declared to be unlawful by this section, including the appointment of a receiver in cases of substantial and willful violation of this section. If a person has acquired moneys or property by and means declared to be unlawful by this section and if the cost of administering reimbursement outweighs the benefit to consumers or consumers entitled to the reimbursement cannot be located through reasonable efforts, the court may order disgorgement of moneys or property acquired by the person by awarding the moneys or property to the state to be used by the attorney general for the administration and implementation of this section. Except in an action for the concealment, suppression, or omission of a material fact with intent that others rely upon it, it is not necessary in an action for reimbursement or an injunction, to allege or prove reliance, damages, intent to deceive, or that the person who engaged in an unlawful act had knowledge of the falsity of the claim or ignorance of the truth. A claim for reimbursement may be proved by any competent evidence, including evidence that would be appropriate in a class action.

In addition to the remedies otherwise provided for in this subsection, the attorney general may request and that court may impose a civil penalty not to exceed $40,000 per violation against a person found by the court to have engaged in a method, act, or practice declared unlawful under this section; provided, however, a course of conduct shall not be considered to be separate and different violations merely because the conduct is repeated to more than one person. In addition, on the motion of the attorney general or on its own motion, the court may impose a civil penalty of not more than $5,000 for each day of intentional violation of a temporary restraining order, preliminary injunction, or permanent injunction issued under authority of this section. A penalty imposed pursuant to this subsection is in addition to any penalty imposed pursuant to 537.6113. Civil penalties ordered pursuant to this subsection shall be paid to the treasurer of state to be deposited in the general fund of the state.

ARE THERE ANY DATA SECURITY REQUIREMENTS IMPOSED?

Section 279.71 requires that the operator of an Internet site, online service, online application, or mobile application with actual knowledge that the site, service, or application is used primarily for kindergarten through grade twelve school purposes and was designed and marketed for such purposes implement and maintain security procedures and practices consistent with current industry standards and all applicable state and federal laws, rules, and regulations appropriate to the nature of the covered information designed to protect that covered information from unauthorized access, destruction, use, modification, or disclosure.

ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

Under § 533.331, a state credit union shall maintain an information security response program that includes procedures for notifying the credit union division as soon as possible after the credit union becomes aware of an incident involving unauthorized access to or use of sensitive member information that would permit access to the member's account.

KANSAS

STATUTE: Kan. Stat. § § **50-7a01** ***et seq.,***[35] **72-6318**.[36]

WHO MUST COMPLY?

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

"Person" means any individual, partnership, corporation, trust, estate, cooperative, association, government, or governmental subdivision or agency or other entity.

WHAT DATA IS COVERED?

Under § 50-7a01(g), personal information is covered. "Personal information" means a consumer's first name or first initial and last name linked to any one or more of the following data elements that relate to the consumer, when the data elements are neither encrypted nor redacted:

(1) social security number;

(2) driver's license number or state identification card number; or

(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 a consumer's financial account.

"Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state or local government records.

WHAT CONSTITUTES A DATA BREACH?

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

"Consumer" means an individual who is a resident of Kansas.

Good faith acquisition of personal information by an employee or agent of an individual or a commercial entity for the purposes of the individual or the commercial entity is not a breach of

[35] Publicly available at: *Consumer information; security breach; definitions*, http://www.kslegislature.org/li_2014/b2013_14/statute/050_000_0000_chapter/050_007a_0000_article/ (last visited June 12, 2019).
[36] Publicly available at: *Kansas Office of Revisor of Statutes*, www.ksrevisor.org, http://www.ksrevisor.org/statutes/chapters/ch72/072_063_0018.html (last visited June 12, 2019).

the security of the system, provided that the personal information is not used for or is not subject to further unauthorized disclosure.

WHO MUST BE NOTIFIED?

The affected Kansas resident and the owner or licensee of the information must be notified.

In the event that a person discovers circumstances requiring notification pursuant to this section of more than 1,000 consumers at one time, the person shall also notify, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by 15 U.S.C. § 1681a(p), of the timing, distribution and content of the notices.

WHEN MUST NOTICE BE SENT?

Notice must be sent as soon as possible following discovery of a breach, if the personal information was, or is reasonably believed to have been, accessed and acquired by an unauthorized person. It should 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.

Notice to the owner or licensee of information must be made following discovery of a breach if personal information was, or is reasonably believed to have been, accessed and acquired by an unauthorized person.

Notice to all consumer reporting agencies, if required, must be made without unreasonable delay.

IN WHAT FORM AND MANNER MUST NOTICE BE SENT?

Notice must be sent in the following manner:

(1) written notice;

(2) electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001; or

(3) substitute notice, if the individual or the commercial entity required to provide notice demonstrates that the cost of providing notice will exceed $100,000, or that the affected class of consumers to be notified exceeds 5,000, or that the individual or the commercial entity does not have sufficient contact information to provide notice.

“Substitute notice” means:

(1) email notice if the individual or the commercial entity has email addresses for the affected class of consumers;

(2) conspicuous posting of the notice on the web site page of the individual or the commercial entity if the individual or the commercial entity maintains a web site; and

(3) notification to major statewide media.

WHAT MUST THE NOTICE SAY?

No specific requirements. The notice must simply carry out its purpose of notifying affected individuals of the breach.

Notice to consumer reporting agencies must include the timing, distribution, and content of the notices sent to affected Kansas residents.

ARE THERE ANY EXEMPTIONS?

Notice may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation. Notice shall be made in good faith, without unreasonable delay and as soon as possible after the law enforcement agency determines that notification will no longer impede the investigation.

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

An individual or a commercial entity that is regulated by state or federal law and that maintains procedures for a breach of the security of the system pursuant to the laws, rules, regulations, guidances, or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance with this section. However, this does not relieve an individual or a commercial entity from a duty to comply with other requirements of state and federal law regarding the protection and privacy of personal information.

WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

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.

ARE THERE ANY DATA SECURITY REQUIREMENTS IMPOSED?

Under K.S. § 50-6,139b, a holder of personal information shall:

(1) implement and maintain reasonable procedures and practices appropriate to the nature of the information, and exercise reasonable care to protect the personal information from unauthorized access, use, modification or disclosure. If federal

or state law or regulation governs the procedures and practices of the holder of personal information for such protection of personal information, then compliance with such federal or state law or regulation shall be deemed compliance with this paragraph and failure to comply with such federal or state law or regulation shall be prima facie evidence of a violation of this paragraph; and

(2) unless otherwise required by federal law or regulation, take reasonable steps to destroy or arrange for the destruction of any records within such holder's custody or control containing any person's personal information when such holder no longer intends to maintain or possess such records. Such destruction shall be by shredding, erasing or otherwise modifying the personal identifying information in the records to make it unreadable or undecipherable through any means.

ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

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.

Section 72-6318 imposes requirements for student data. In the event of a security breach or unauthorized disclosure of student data or personally identifiable information of any student, whether by a school district, the department, the state board of education, state agency, or other entity or third party given access to student data or personally identifiable information on any student, the school district, department, state board of education, state agency, or other entity or third party shall immediately notify each affected student, if an adult, or the parent or legal guardian of the student, if a minor, of the breach or unauthorized disclosure and investigate the causes and consequences of the breach or unauthorized disclosure.

KENTUCKY

STATUTE: Ky. Rev. Stat. §§ 365.732,[37] 365.730,[38] 61.931-61.934.[39]

WHO MUST COMPLY?

A person or business entity that conducts business in the State and which owns, licenses, or maintains computerized data that includes personal information about a Kentucky resident. Ky. Rev. Stat. § 365.732(1)(b).

WHAT DATA IS COVERED?

An individual's first name or first initial and last name, in addition to one or more of the following: (1) Social Security number; (2) driver's license number; or (3) account number or credit or debit card number, in combination with any required security code, access code, or password to permit access to an individual's financial account. Ky. Rev. Stat. § 365.732(1)(c).

WHAT CONSTITUTES A DATA BREACH?

Unauthorized acquisition of unencrypted and un-redacted computerized data that compromises the security, confidentiality, or integrity of personally identifiable information maintained by the information holder as part of a database regarding multiple individuals that actually causes, or leads the information holder to reasonably believe has caused or will cause, identity theft or fraud against any resident of the Commonwealth of Kentucky. Good-faith acquisition of personally identifiable information by an employee or agent of the information holder for the purposes of the information holder is not a breach of the security of the system if the personally identifiable information is not used or subject to further unauthorized disclosure. Ky. Rev. Stat. § 365.732(1)(a).

The statute does not apply if the data subject to the breach is encrypted or redacted. Ky. Rev. Stat. § 365.732(1)(a). The statute does not define encryption.

WHO MUST BE NOTIFIED?

Any resident of Kentucky whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Ky. Rev. Stat. § 365.732(2).

If the breach affects a person that maintains or stores covered information, that person must notify the owner or licensee of that information. Ky. Rev. Stat. § 365.732(3).

If a person discovers circumstances requiring notification pursuant to this section of more than 1,000 persons at one time, the person shall also notify, without unreasonable delay, all consumer

[37] Publicly available at: *365.732*, www.lrc.ky.gov, https://apps.legislature.ky.gov/law/statutes/statute.aspx?id=43326 (last visited May 28, 2019).
[38] Publicly available at: *365.730*, www.lrc.ky.gov, https://apps.legislature.ky.gov/law/statutes/statute.aspx?id=34844 (last visited May 28, 2019).
[39] Publicly available at: *61.931*, www.lrc.ky.gov, https://apps.legislature.ky.gov/law/statutes/statute.aspx?id=43575 (last visited May 28, 2019).

reporting agencies and credit bureaus that compile and maintain files on consumers on a nationwide basis, as defined by 15 U.S.C. § 1681a, of the timing, distribution, and content of the notices. Ky. Rev. Stat. § 365.732(7).

WHEN MUST NOTICE BE SENT?

The disclosure shall be made in the most expedient time possible, following discovery or notification of the breach, and without unreasonable delay, consistent with the legitimate needs of law enforcement. Ky. Rev. Stat. § 365.732(2).

IN WHAT FORM AND MANNER MUST NOTICE BE SENT?

In one of the following manners: (1) written notice; (2) electronic notice, if consistent with 15 U.S.C. § 7001; or (3) substitute notice, if the information holder demonstrates that the cost of providing notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000, or the information holder does not have sufficient contact information.

Substitute notice shall consist of all of the following:

(1) e-mail notice, when the information holder has an e-mail address for the subject persons;

(2) conspicuous posting of the notice on the information holder's Internet website page, if the information holder maintains a website page; and

(3) notification to major Statewide media.

Ky. Rev. Stat. § 365.732(5).

WHAT MUST THE NOTICE SAY?

The statute does not address the contents of the notification.

ARE THERE ANY EXEMPTIONS?

Notwithstanding subsection (5) of this section, an information holder that maintains its own notification procedures as part of an information security policy for the treatment of personally identifiable information, and is otherwise consistent with the timing requirements of this section, shall be deemed to be in compliance with the notification requirements of this section, if it notifies subject persons in accordance with its policies in the event of a breach of security of the system. Ky. Rev. Stat. § 365.732(6).

The provisions of this section and the requirements for non-affiliated third-parties in Ky. Rev. Stat. Chapter 61 shall not apply to any person who is subject to the provisions of Title V of the Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, as amended, or the federal Health Insurance Portability and Accountability Act ("HIPAA") of 1996, Pub. L. No. 104-191, as amended, or any agency of the Commonwealth of Kentucky or any of its local governments or political subdivisions. Ky. Rev. Stat. § 365.732(8).

Back to TOC

WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

Any customer injured by a violation of § 365.725 may institute a civil action to recover damages and the violator's business may be enjoined. A cloud computing service provider shall not process student data for any purpose other than providing, improving, developing, or maintaining the integrity of its cloud computing services, unless the provider receives express permission from the student's parent. Ky. Rev. Stat. § 365.730(1).

ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

None.

LOUISIANA

STATUTE: La. Rev. Stat. § 51:3071 et seq.,[40] 40:1173.1-1173.6,[41] La. Admin. Code Title 16, pt. III, § 701.[42]

WHO MUST COMPLY?

Any person or agency that owns or licenses computerized data that includes personal information regarding a Louisiana resident or any person or agency that maintains computerized data that includes personal information that the person or agency does not own. La. Rev. Stat. §§ 51:3074(A), 51:3074(B).

WHAT DATA IS COVERED?

The first name or first initial and last name of an individual resident of the State in combination with any one or more of the following data elements, when the name or the data element is not encrypted or redacted:

(1) Social Security number;

(2) driver's license number or State 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;

(4) passport number; or

(5) biometric data, defined as data generated by automatic measurements of an individual's biological characteristics, such as fingerprints, voice print, eye retina or iris, or other unique biological characteristics used by the owner or licensee to authenticate an individual's identity when the individual accesses a system or account.

Covered data shall not include publicly available information that is lawfully made available to the general public from federal, State, or local government records. La. Rev. Stat. § 51:3073(4)(b).

---

[40] Publicly available at: *Louisiana State Legislature*, www.legis.la.gov, http://legis.la.gov/Legis/Law.aspx?p=y&d=322027 (last visited May 29, 2019). The statute was amended by Act. No. 382, enacted on May 20, 2018 and effective Aug. 1, 2018 (publicly available at https://www.legis.la.gov/legis/ViewDocument.aspx?d=1101149 (last visited May 29, 2019)).

[41] Publicly available at: *Louisiana State Legislature*, www.legis.la.gov, http://legis.la.gov/Legis/Law.aspx?d=964730 (last visited May 29, 2019). The statute was amended by Act. No. 206, enacted May 15, 2018 and effective August 1, 2018, but the changes were technical and non-substantive.

[42] Publicly available at: *Online Publications of the Louisiana Administrative Code*, www.doa.la.gov, http://www.doa.la.gov/pages/osr/lac/books.aspx (last visited May 29, 2019).

WHAT CONSTITUTES A DATA BREACH?

The compromise of the security, confidentiality, or integrity of computerized data that results in, or there is a reasonable likelihood to result in, the unauthorized acquisition of and access to personal information maintained by an agency or person. Good faith acquisition of personal information by an employee or agent of an agency or person for the purposes of the agency or person is not a breach of the security of the system, provided that the personal information is not used for, or is subject to, unauthorized disclosure. La. Rev. Stat. § 51:3073(2).

WHO MUST BE NOTIFIED?

Any resident of Louisiana whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person. La. Rev. Stat. § 51:3074(C).

If the breach affects an agent or person that maintains or stores covered information, that agent or person must notify the owner or licensee of that information. La. Rev. Stat. § 51:3074(D).

If notice to affected residents is required, written notice must also be provided to the Consumer Protection Section of the Attorney General's Office. Such notice must detail the security breach and include the names of all residents affected by the breach. La. Admin. Code tit. 16, pt. III, § 701.

Notification is not required if after a reasonable investigation the person or business determines that there is no reasonable likelihood of harm to the residents of Louisiana. La. Rev. Stat. § 51:3074(I).

WHEN MUST NOTICE BE SENT?

The notification to any affected resident or the owner or licensee of personal information that has been compromised shall be made in the most expedient time possible and without unreasonable delay, but not later than 60 days from the discovery of the breach, consistent with the legitimate needs of law enforcement, or any measures necessary to determine the scope of the breach, prevent further disclosures, and restore the reasonable integrity of the data system. La. Rev. Stat. § 51:3074(E).

When a law enforcement agency determines that the notification required would impede a criminal investigation, such notification may be delayed until such agency determines the notification will no longer compromise the investigation. La. Rev. Stat. § 51:3074(F).

When the notification required is delayed by a law enforcement agency or a determination by a person or agency that measures are necessary to determine the scope of the breach, prevent further disclosures, and restore the reasonable integrity of the data system, the person or agency shall provide the attorney general the reasons for the delay in writing within the 60-day notification period. Upon receipt of the written reasons, the attorney general shall allow a reasonable extension of time to provide the notification required. La. Rev. Stat. § 51:3074(E)-(F).

Notice to the attorney general is timely if it is received within 10 days of distribution of notice to Louisiana citizens. La. Admin. Code 16, pt. III, § 701(B).

IN WHAT FORM AND MANNER MUST NOTICE BE SENT?

Notification must be provided by one of the following methods:

(1) written notification;

(2) electronic notification, if the notification provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001; or

(3) substitute notification, if the notifying agency or person demonstrates that the cost of providing notification would exceed $100,000, or that the affected class of persons to be notified exceeds 100,000, or the agency or person does not have sufficient contact information.

Substitute notification shall consist of all of the following:

(1) e-mail notification when the agency or person has an e-mail address for the subject persons;

(2) conspicuous posting of the notification on the website of the agency or person, if a website is maintained; and

(3) notification to major Statewide media.

La. Rev. Stat. § 51:3074(G).

WHAT MUST THE NOTICE SAY?

The statute does not address the contents of the notification.

ARE THERE ANY EXEMPTIONS?

Notification is not required if after a reasonable investigation the person or business determines that there is no reasonable likelihood of harm to the residents of Louisiana. The person or business must retain a copy of the written determination and supporting documentation for 5 years from the date of discovery of the breach. If requested in writing, the person or business shall send a copy of the written determination and supporting documentation to the attorney general no later than 30 days from receipt of the request. La. Rev. Stat. § 51:3074(I).

An agency or person that maintains a notification procedure as part of its information security policy for the treatment of personal information which is otherwise consistent with the timing requirements of La. Rev. Stat. § 51:3074 shall be considered to be in compliance with the notification requirements of § 51:3074 if the agency or person notifies subject persons in

accordance with such policy and procedure in the event of a breach of security of the system. La. Rev. Stat. § 51:3074(H).

A financial institution that is subject to and in compliance with the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, issued on March 7, 2005, by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency and the Office of Thrift Supervision, and any revisions, additions, or substitutions relating to the Interagency Guidance, shall be deemed to be in compliance with this Chapter. La. Rev. Stat. § 51:3076.

WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

A civil action may be instituted by an affected customer to recover actual damages resulting from the failure to disclose in a timely manner that there has been a breach of the security system resulting in the disclosure of a person's personal information. La. Rev. Stat. § 51:3075.

Any violation of the statute will be deemed an unfair act or practice pursuant to La. Rev. Stat. § 51:1405(a). La. Rev. Stat. § 51:3075(J).

Restraining Prohibited Acts: The attorney general may bring an action for injunctive relief and request the court impose a civil penalty against any person found by the court to have engaged in a violation of the statute. La. Stat. Ann. § 51:1407(A)-(B). In the event the court finds the violation was done with the intent to defraud, the court may impose a penalty not to exceed $5,000 for each violation. La. Stat. Ann. § 51:1407(B). Additionally, if the violation was committed against an elder person or a person with a disability, the court may impose an additional civil penalty not to exceed $5,000 for each violation. La. Stat. Ann. § 51:1407(C).

Additional Relief: The court may also order any relief as may be necessary to compensate any aggrieved person including but not limited to: (1) revocation, forfeiture, or suspension of any license, charter, franchise, certificate, or other evidence of authority of any person to do business in the State; (2) dissolution of domestic corporations or associations; (3) suspension or termination of the right of foreign corporations or associations to do business in this State; or (4) restitution. La. Stat. Ann. § 51:1408(A).

Private Actions: Any person who suffers any ascertainable loss of money or movable property as a result of a violation of the statute may bring an action individually to recover actual damages. After being put on notice by the attorney general, the court shall award three times the actual damages sustained if it finds the violation was done knowingly. In the event damages are awarded in a private action, the court will award to the person brining such action reasonable attorney fees and costs. La. Stat. Ann. § 51:1409(A).

Failure to provide timely notice to the attorney general may be punishable by a fine not to exceed $5,000 per violation. Each day notice is not received shall be deemed a separate violation. La. Admin. Code tit. 16, pt. III, § 701(B).

ARE THERE ANY DATA SECURITY REQUIREMENTS IMPOSED?

Any person that conducts business in the State or that owns or licenses computerized data that includes personal information, or any agency that owns or licenses computerized data that includes personal information: (1) shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information from unauthorized access, destruction, use, modification, or disclosure; and (2) shall take all reasonable steps to destroy or arrange for the destruction of the records within its custody or control containing personal information that is no longer to be retained by the person or business by shredding, erasing, or otherwise modifying the personal information in the records to make it unreadable or undecipherable through any means. La Rev. Stat. 51:3074(A)-(B).

ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

The Louisiana Department of Health must comply with La. Rev. Stat. §§ 40:1173.1 through 40:1173.6, which requires the Department to maintain any computerized database of personal health information of consumers in a secure environment in compliance with federal laws providing for the security of the system containing such data and to notify within 30 days of a known or suspected breach each resident of the State whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person. La. Rev. Stat. § 40:1173.3(6). Penalties for violations are set forth in La. Rev. Stat. § 40:1173.6.

MAINE

STATUTE: Me. Rev. Stat. Ann. 10 § 1346 *et seq.*[43]

WHO MUST COMPLY?

Information brokers, any persons, and third-party entities that maintain computerized data that includes personal information of Maine residents. Me. Rev. Stat. tit. 10, § 1348.

Information broker is defined as any person who, for monetary fees or dues, engages in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring or communicating information concerning Maine residents for the primary purpose of furnishing personal information to nonaffiliated third-parties. This definition does not include a governmental agency whose records are maintained primarily for traffic safety, law enforcement or licensing purposes. Me. Rev. Stat. Ann. 10 § 1347(3).

WHAT DATA IS COVERED?

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

(1) Social Security number;

(2) driver's license number or State identification card number;

(3) account number, credit card number or debit card number, if circumstances exist wherein such a number could be used without additional identifying information, access codes or passwords;

(4) account passwords or personal identification numbers or other access codes; or

(5) any of the data elements contained in paragraphs (1) to (4) when not in connection with the individual's first name, or first initial, and last name, if the information if compromised would be sufficient to permit a person to fraudulently assume or attempt to assume the identity of the person whose information was compromised.

This data does not include information from third-party claims databases maintained by property and casualty insurers or publicly available information that is lawfully made available to the general public from federal, State or local government records or widely distributed media. Me. Rev. Stat. Ann. 10 § 1347(6).

[43] Publicly available at: *Maine Revised Statutes*, www.legislature.maine.gov, http://legislature.maine.gov/statutes/10/title10ch210-Bsec0.html (last visited May 29, 2019).

WHAT CONSTITUTES A DATA BREACH?

Unauthorized acquisition, release or use of an individual's computerized data that includes personal information that compromises the security, confidentiality or integrity of personal information of the individual maintained by a person.

Good faith acquisition, release or use of personal information by an employee or agent of a person on behalf of the person is not a breach of the security of the system if the personal information is not used for or subject to further unauthorized disclosure to another person. Me. Rev. Stat. Ann. 10 § 1347(1).

WHO MUST BE NOTIFIED?

In the case of a breach of the security of a system maintained by an information broker, the information broker must conduct a good-faith, reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused and notify any Maine resident whose personal information has been, or is reasonably believed to have been, acquired by an unauthorized person. Me. Rev. Stat. Ann. 10 § 1348(1).

In the case of a breach of the security of a system maintained by any other person, the person must conduct a good-faith, reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused and notify any Maine resident if personal information has been misused or if it is reasonably possible such misuse will occur. Me. Rev. Stat. Ann. 10 § 1348(1).

A third-party entity that maintains, on behalf of a person, computerized data that includes personal information that the third-party entity does not own shall notify the person maintaining personal information of a breach of the security of the system immediately following discovery if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Me. Rev. Stat. Ann. 10 § 1348(2).

When notice of a breach of the security of the system is required to be made to affected residents or persons maintaining personal information that has been compromised, the person shall notify the appropriate State regulators within the Department of Professional and Financial Regulation, or if the person is not regulated by the Department, the Attorney General. Me. Rev. Stat. Ann. 10 § 1348(5).

If a person discovers a breach of the security of the system that requires notification to more than 1,000 persons at a single time, the person shall also notify, without unreasonable delay, consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. § 1681a(p). Notification must include the date of the breach, an estimate of the number of persons affected by the breach, if known, and the actual or anticipated date that persons were or will be notified of the breach. Me. Rev. Stat. Ann. 10 § 1348(4).

WHEN MUST NOTICE BE SENT?

Notices must be made as expediently as possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or with measures necessary to determine the scope of

the security breach and restore the reasonable integrity, security and confidentiality of the data in the system. Me. Rev. Stat. Ann. 10 § 1348(1).

The statute's notification requirements may be delayed for no longer than 7 business days after a law enforcement agency determines that the notification will not compromise a criminal investigation. Me. Rev. Stat. Ann. 10 § 1348(3).

A third-party entity that maintains computerized data that includes personal information that the third-party entity does not own must provide required notification of a breach immediately following discovery. Me. Rev. Stat. Ann. 10 § 1348(2).

IN WHAT FORM AND MANNER MUST NOTICE BE SENT?

The notice must be: (1) written notice; (2) electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001; or (3) substitute notice, if the person maintaining personal information demonstrates that the cost of providing notice would exceed $5,000, that the affected class of individuals to be notified exceeds 1,000, or that the person maintaining personal information does not have sufficient contact information to provide written or electronic notice to those individuals.

Substitute notice must consist of all of the following:

(1) e-mail notice, if the person has e-mail addresses for the individuals to be notified;

(2) conspicuous posting of the notice on the person's publicly accessible website, if the person maintains one; and

(3) notification to major Statewide media.

Me. Rev. Stat. Ann. 10 § 1347(4).

WHAT MUST THE NOTICE SAY?

The statute does not address the contents of the notification.

ARE THERE ANY EXEMPTIONS?

A person that complies with the security breach notification requirements of rules, regulations, procedures or guidelines established pursuant to federal law or the laws of Maine is deemed to be in compliance with the requirements of § 1348 as long as the law, rules, regulations or guidelines provide for notification procedures at least as protective as that provision's notification requirements. Me. Rev. Stat. Ann. 10 § 1349(4).

WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

The appropriate State regulators within the Department of Professional and Financial Regulation are responsible for enforcing the statute with respect to any person that is licensed or regulated

by those regulators. The State attorney general shall enforce this chapter for all other persons. Me. Rev. Stat. Ann. 10 § 1349(1).

The statute provides for (1) civil penalties up to $500 per violation, up to a maximum of $2,500 for each day a person is in violation of the statute (except that this does not apply to State Government, the University of Maine System, the Maine Community College System or Maine Maritime Academy); (2) equitable relief; and (3) injunction from further violations. Me. Rev. Stat. Ann. 10 § 1349(2).

ARE THERE ANY DATA SECURITY REQUIREMENTS IMPOSED?

No.

ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

The Maine Bureau of Insurance issued Bulletin 345, which clarifies that the notification statute also applies to persons and entities licensed or regulated by the Superintendent, such as insurers, producers, adjusters, and third-party administrators. These entities must also notify the Superintendent, under § 1348(5), of breaches that require notice under § 1348(1). In addition to the information required by § 1348(4) and mentioned in the previous paragraph, the notice to the Superintendent should include a description of the breach, the number of Maine residents affected by the breach, if known, a copy of the notice and other information sent to affected persons, a description of other curative steps taken, and the name and contact information for the person whom the Superintendent may contact about the breach.

MARYLAND

STATUTE: Md. Code, Com. Law § 13-401, *et seq.*;[44] Md. Code, Com. Law § 14-3501, *et seq.*;[45] Md. Code, State Gov't. §§ 10-1301-1308.[46]

WHO MUST COMPLY?

A business that owns, maintains or licenses computerized data that includes personal information of an individual residing in Maryland. Md. Code, Com. Law §§ 14-3504(b), 14-3504(c).

"Business" is defined as any sole proprietorship, partnership, corporation, association, or any other business entity, whether or not organized to operate at a profit, including a financial institution organized, chartered, licensed, or otherwise authorized under the laws of any State, the United States, or any other country, and the parent or subsidiary of a financial institution. Md. Code, Com. Law § 14-3501(b).

WHAT DATA IS COVERED?

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 or the data elements are not encrypted, redacted, or otherwise protected by another method that renders the information unreadable or unusable:

(1) Social Security number, an Individual Taxpayer Identification Number, a passport number, or other identification number issued by the federal government;

(2) driver's license number or State identification card number;

(3) an account number, a credit card number, or a debit card number, that in combination with any required security code, access code, or password, would permit access to an individual's financial account;

---

[44] Publicly available at: *General Assembly of Maryland*, http://mgaleg.maryland.gov/webmga/frmStatutesText.aspx?article=gcl&section=13-410&ext=html&session=2019RS&tab=subject5 (last visited June 7, 2019). Maryland's Financial Consumer Protection Act of 2018, enacted on May 15, 2018 and effective Oct. 1, 2018, will increase penalty caps to $10,000 for each violation and $25,000 for each subsequent act repeating the same violation. Enacting legislation H.B. 1634 is publicly available at http://mgaleg.maryland.gov/2018RS/bills/hb/hb1634E.pdf (last visited June 7, 2019); the cross-filed S.B. 1068 is publicly available at http://mgaleg.maryland.gov/2018RS/bills/sb/sb1068E.pdf (last visited June 7, 2019).

[45] Publicly available at: *General Assembly of Maryland*, www.mgaleg.maryland.gov, http://mgaleg.maryland.gov/webmga/frmStatutesText.aspx?article=gcl&section=14-3501&ext=html&session=2017RS&tab=subject5 (last visited June 1, 2019). This statute was amended to include "Insurance – Breach of Security of a Computer System – Notification Requirement," enacted S.B. 30 on April 18, 2019 and effective October 1, 2019. Publicly available at: *General Assembly of Maryland*, http://mgaleg.maryland.gov/2019RS/bills/sb/sb0030T.pdf (last visited July 19, 2019). Also, amended to include H.B. 1154, which was enacted on April 30, 2019 and effective October 1, 2019. Publicly available at: *General Assembly of Maryland*, http://mgaleg.maryland.gov/2019RS/bills/hb/hb1154T.pdf (last visited July 19, 2019).

[46] Publicly available at: *General Assembly of Maryland*, www. mgaleg.maryland.gov, http://mgaleg.maryland.gov/2019RS/bills/sb/sb0030T.pdf http://mgaleg.maryland.gov/webmga/frmStatutesText.aspx?article=gsg&section=10-1301&ext=html&session=2018RS&tab=subject5 (last visited June 1, 2019).

(4) any information created by an entity covered by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") regarding an individual's medical history, medical condition, or medical treatment or diagnosis, 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 used by an insurer or self-insured employer, that permits access to an individual's health information; or

(6) biometric data generated by automatic measurements of an individual's biological characteristics such as a fingerprint, voice print, genetic print, retina or iris image, or other unique biological characteristic, that can be used to uniquely authenticate the individual's identity when the individual accesses a system or account; or

(7) a user name or e-mail address in combination with a password or security question and answer that permits access to an individual's e-mail account.

Md. Code, Com. Law § 14-3501(e)(1).

Personal information does not include: (a) publicly available information that is lawfully made available to the general public from federal, State, or local government records; (b) information that an individual has consented to have publicly disseminated or listed; or (c) information that is disseminated or listed in accordance with HIPAA. Md. Code, Com. Law § 14-3501(e)(2).

WHAT CONSTITUTES A DATA BREACH?

Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of the personal information maintained by a business. Breach does not include the good faith acquisition of personal information by an employee or agent of a business for the purposes of the business, provided that the personal information is not used or subject to further unauthorized disclosure. Md. Code, Com. Law § 14-3504(a).

The statute does not apply if the data subject to the breach is personal information under § 14-3501(e)(1)(i) that is encrypted, redacted, or otherwise protected by another method that renders the information unreadable or unusable. "Encrypted" means the transformation of data through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key. Md. Code, Com. Law § 14-3501(c), 14-3501(e)(1)(i).

WHO MUST BE NOTIFIED?

If, after concluding a good-faith, reasonable, and prompt investigation, the business determines that misuse of a Maryland resident's personal information has occurred or is reasonably likely to occur as a result of a breach of the security of a system, the business shall notify the individual of the breach. Md. Code, Com. Law § 14-3504(b).

Prior to providing notice to a Maryland resident, a business shall first provide notice of a breach of the security of a system to the Office of the Attorney General. Md. Code, Com. Law § 14-3504(h).

If after concluding the required investigation, the business determines that notification is not required, the business shall maintain records that reflect its determination for 3 years after the determination is made. Md. Code, Com. Law § 14-3504(b)(4). If the breach affects a business that maintains computerized data that includes personal information of a Maryland resident, that business must notify the owner or licensee of that information. Md. Code, Com. Law § 14-3504(c).

If notification to 1,000 or more individuals is required, the business shall also notify, without unreasonable delay, each consumer reporting agency that compiles and maintains files on consumers on a nationwide basis, as defined by 15 U.S.C. § 1681a(p), of the timing, distribution, and content of the notices. Such notice does not require the inclusion of the names or other personal identifying information of the individual recipients of notices of the breach. Md. Code, Com. Law § 14-3506.

WHEN MUST NOTICE BE SENT?

Notification to affected residents must be given as soon as reasonably practicable, but not later than 45 days after the business conducts a reasonable and prompt investigation and determines that the breach created a likelihood that personal information has been or will be misused. Md. Code, Com. Law § 14-3504(b)(3).

Notification to the owner or licensee of affected personal information by a business that maintains the data must be made as soon as reasonably practicable but not later than 45 days after the business discovers or is notified of the breach. Md. Code, Com. Law § 14-3504(c)(2).

Notification may be delayed by (1) a determination by a law enforcement agency that the notification will impede a criminal investigation or jeopardize homeland or national security, or (2) a need to determine the scope of the breach, identify the individuals affected, or restore the integrity of the system. In the case of a delay by a law enforcement agency, the business shall provide notification as soon as reasonably practicable, but not later than 30 days after the law enforcement agency determines the notification will not impede a criminal investigation nor jeopardize homeland or national security. Md. Code , Com. Law § 14-3504(d)(1)-(2).

IN WHAT FORM AND MANNER MUST NOTICE BE SENT?

Notice must be given:

(1) by written notice sent to the most recent address of the individual in the records of the business;

(2) by electronic mail to the most recent electronic mail address of the individual in the records of the business, if: the individual has expressly consented to receive electronic notice or the business conducts its business primarily through Internet account transactions or the Internet;

(3) by telephonic notice, to the most recent telephone number of the individual in the records of the business; or

(4) by substitute notice if:

(a) the business demonstrates that the cost of providing notice would exceed $100,000, or that the affected class of individuals to be notified exceeds 175,000; or

(b) the business does not have sufficient contact information to give notice in accordance with (i), (ii), or (iii) above.

Md. Code, Com. Law § 14-3504(e).

Substitute notice shall consist of: (1) electronically mailing the notice to an individual entitled to notification, if the business has an e-mail address for the individual to be notified; (2) conspicuous posting of the notice on the website of the business, if the business maintains one; and (3) notification to Statewide media. Md. Code, Com. Law § 14-3504(f).

WHAT MUST THE NOTICE SAY?

Except for breaches involving personal information that permits access to an e-mail account only and no other personal information, the notification shall include:

(1) to the extent possible, a description of the categories of information that were, or are reasonably believed to have been, acquired by an unauthorized person, including which of the elements of personal information were, or are reasonably believed to have been, acquired;

(2) contact information for the business making the notification, including the business's address, telephone number, and toll-free telephone number;

(3) the toll-free telephone numbers and addresses for the major consumer reporting agencies; and

(4) the toll-free telephone numbers, addresses, and Web site addresses for: (1) the Federal Trade Commission; and (2) the Office of the Attorney General; and

(5) a statement that an individual can obtain information from the Federal Trade Commission and the Office of the Attorney General about steps the individual can take to avoid identity theft.

Md. Code, Com. Law § 14-3504(g).

If the breach involves personal information that permits access to an individual's e-mail account only, and affects no other personal information, the business may comply with the notification requirement by providing notification in electronic or other form that directs the individual whose personal information has been breached to promptly: (a) change the individual's password

and security question or answer as applicable; or (b) take other steps appropriate to protect the e-mail account with the business and all other online accounts for which the individual uses the same username or e-mail address and password or security question or answer. Notification may be provided by e-mail to the e-mail account affected by the breach only by clear and conspicuous notice delivered to the individual online while the individual is connected to the affected e-mail account from an Internet Protocol address or online location from which the business knows the individual customarily accesses the account. Md. Code, Com. Law § 14-3504(i).

ARE THERE ANY EXEMPTIONS?

A business that complies with the requirements for notification procedures, the protection or security of personal information, or the destruction of personal information under the rules, regulations, procedures, or guidelines established by the primary or functional federal or State regulator of the business shall be deemed to be in compliance with the statute. Md. Code, Com. Law § 14-3507(b).

A business or affiliate that is subject to and in compliance with: (1) § 501(b) of the federal Gramm-Leach-Bliley Act; (2) § 216 of the federal Fair and Accurate Credit Transactions Act; (3) the federal Interagency Guidelines Establishing Information Security Standards; (4) the federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, and any revisions, additions, or substitutions thereto; and (5) HIPAA shall be deemed to be in compliance with the statute. Md. Code, Com. Law § 14-3507(c)-(d).

WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

A violation of the statute shall constitute an unfair or deceptive trade practice under Maryland law. Md. Code, Com. Law § 14-3508.

An injured person may institute a private action to recover actual damages. Md. Code, Com. Law § 13-408(a).

The State attorney general has enforcement authority for the statute and may seek: (1) injunctive relief; (2) in the case of a "merchant" as defined at Md. Code, Com. Law § 13-101, (A) a civil penalty of not more than $1,000 for each violation, and (B) a civil penalty of not more than $5,000 for each subsequent act repeating the same violation; and (3) costs of the action. Md. Code, Com. Law §§ 13-406, 13-409, 13-410. Effective October 1, 2018, violators are subject to a civil penalty of not more than $10,000 for each violation and a civil penalty of not more than $25,000 for each subsequent act repeating the same violation.

The Consumer Protection Division shall consider the following in setting the amount of the penalty:

(1) the severity of the violation for which the penalty is assessed;

(2) the good faith of the violator;

(3) any history of prior violations;

(4) whether the amount of the penalty will achieve the desired deterrent purpose; and

(5) whether the issuance of a cease and desist order, including restitution, is insufficient for the protection of consumers.

Md. Code, Com. Law § 13-410.

Any person who violates any provision of this title is guilty of a misdemeanor and, unless another criminal penalty is specifically provided elsewhere, on conviction is subject to a fine not exceeding $1,000 or imprisonment not exceeding one year or both, in addition to any civil penalties. Md. Code, Com. Law § 13-411.

ARE THERE ANY DATA SECURITY REQUIREMENTS IMPOSED?

When a business is destroying a customer's, an employee's, or a former employee's records that contain personal information of the customer, employee, or former employee, 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.

Md. Code Ann., Com. Law § 14-3502(b).

A business that owns or licenses personal information of a resident shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal information owned or licensed and the nature and size of the business and its operations. Md. Code Ann., Com. Law § 14-3503(a).

A business that uses a nonaffiliated third party as a service provider to perform services for the business and discloses personal information about a resident under a written contract with the third party shall require by contract that the third party implement and maintain reasonable security procedures and practices that: (i) are appropriate to the nature of the personal information disclosed to the nonaffiliated third party; and (ii) are reasonably designed to help protect the personal information from unauthorized access, use, modification, disclosure, or destruction. This applies only to a written contract entered into on or after January 1, 2009. Md. Code Ann., Com. Law § 14-3502(b).

ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

Health Information:

A Health Information Exchange ("HIE") is an entity that creates or maintains an infrastructure that provides organizational and technical capabilities in an interoperable system for the electronic exchange of protected health information among participating organizations not under common ownership, in a manner that ensures the secure exchange of protected health information to provide care to patients. COMAR 10.25.18.02(B)(27).

Among the requirements for maintaining health information set forth in COMAR 10.25.18.01-12, an HIE must conduct an investigation (not to exceed 14 business days) if it has a reasonable belief that a breach or non-HIPAA violation has occurred. An HIE must notify the Maryland Health Care Commission ("Commission") within 10 business days of acquiring a reasonable belief that a non-HIPAA violation or breach under HIPAA has occurred, either as a result of an investigation or otherwise. COMAR 10.25.18.07. The Commission must forward notification of a breach to the attorney general within 30 days of receipt.

The HIE shall notify a health care consumer, if such notification is required under applicable law, including HIPAA, or if so directed by the Commission due to the seriousness of the non-HIPAA violation. COMAR 10.25.18.07(C)(4). The notification must be in writing within a reasonable time frame, but not later than 60 days from the discovery of the breach or from the date that the HIE should have reasonably discovered the breach. COMAR 10.25.18.08(C)(4). The written notification shall include:

(1) a description of the breach or non-HIPAA violation that occurred and the remedial actions taken by the participating organization, provided that the notification shall not contain any sensitive health information;

(2) information about the patient's right to notify credit reporting agencies of the potential for identity theft or medical identity theft;

(3) contact information for the HIE, including the address and toll-free telephone number where the health care consumer can learn more information;

(4) contact information for at least one credit reporting agency;

(5) information concerning the patient's right to opt out of the HIE; and

(6) the toll-free numbers, addresses, and websites for:

(A) the Office of the Attorney General, Consumer Protection Division; and

(B) the U.S. Department of Health and Human Services, Office of Civil Rights.

If the entity providing the notification keeps a medical record on the patient, the notification shall be placed within the patient's medical record. COMAR 10.25.18.08(C)(5).

State Entities:

Md. Code, State Gov't. §§ 10-1301 through 10-1308 set forth specific requirements for notification in the event of a breach, security procedures and practices to protect personal information, and destruction of records containing personal information applicable to: (1) any executive agency, or a department, a board, a commission, an authority, a public institution of higher education, a unit or an instrumentality of the State; or (2) any county, municipality, bi-county, regional, or multicounty agency, county board of education, public corporation or authority, or any other political subdivision of the State. These requirements do not apply to Maryland's legislative or judicial branch.

Insurance:

Effective October 1, 2019, "carriers" will be required "to notify the Maryland Insurance Commissioner . . . that a certain breach of the security of a system has occurred;" and provide notice of the breach within 45 days.

"Carrier" is defined as: (i) an insurer; (ii) a non-profit health service plan; (iii) a health maintenance organization; (iv) a dental organization; (v) a managed general agent; or (vi) a third-party administrator.

Compliance with this section does not relieve a Carrier from a duty to comply with any other requirements of Federal law or Title 14 of the Commercial Law Article relating to the protection and privacy of personal information.

Md. Code Ann., Com. Law § 4-406 (amended by S.B. 30).

Non-Owner/Licensee/Vendor:

If the breached business is not the "owner or licensee of the computerized data, the business may not charge the owner or licensee of the computerized data a fee for providing information that the owner or licensee needs to make a notification under" the statute, and the "owner or licensee of the computerized data may" only use the information relative to the breach to (1) provide notification of the breach, (2) protect or secure personal information, or (3) provide notification to national information security organizations created for information-sharing and analysis of security threats to avert additional breaches.

Md. Code Ann., Com. Law § 14-3504 (amended by H.B. 1154).

MASSACHUSETTS

STATUTE: Mass. Gen Laws. **Ch. 93A § 4**;[47] **93H § 1 *et seq.*;**[48] and **93I § 1 et seq**.[49] Mass. Regs. Code **Tit. 201, § 17.01 et seq**.[50]

WHO MUST COMPLY?

A person or agency that maintains, stores, owns, or licenses data that includes personal information about a resident of Massachusetts. Mass. Gen Laws. Ch. 93H § 3(a)-(b).

An agency is defined as any executive office, department, board, commission, bureau, division or authority of Massachusetts, or any of its branches or political subdivisions. Mass. Gen Laws. Ch. 93H § 1(a).

WHAT DATA IS COVERED?

A resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident:

(1) Social Security number;

(2) driver's license number or State-issued identification card number; or

(3) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account.

This does not include information that is lawfully obtained from publicly available information, or from federal, State or local government records lawfully made available to the general public. Mass. Gen Laws. Ch. 93H § 1(a).

WHAT CONSTITUTES A DATA BREACH?

Unauthorized acquisition or unauthorized use of unencrypted data or encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of Massachusetts. Mass. Gen Laws. Ch. 93H § 1(a).

---

[47] Publicly available at: *The 190th General Court Of The Commonwealth Of Massachusetts*, www.malegislature.gov, https://malegislature.gov/Laws/GeneralLaws/PartI/TitleXV/Chapter93A/Section4 (last visited June 7, 2019).
[48] Publicly available at: *The 190th General Court Of The Commonwealth Of Massachusetts*, www.malegislature.gov, https://malegislature.gov/Laws/GeneralLaws/PartI/TitleXV/Chapter93h/Section1 (last visited June 7, 2019).
[49] Publicly available at: *The 190th General Court Of The Commonwealth Of Massachusetts*, www.malegislature.gov, https://malegislature.gov/Laws/GeneralLaws/PartI/TitleXV/Chapter93i/Section1 (last visited June 7, 2019).
[50] Publicly available at www.mass.gov, https://www.mass.gov/files/documents/2017/10/02/201cmr17.pdf (last visited June 7, 2019).

A good faith but unauthorized acquisition of personal information by a person or agency, or employee or agent thereof, for lawful purposes, does not constitute a breach unless the personal information is used in an unauthorized manner or subject to further unauthorized disclosure. Mass. Gen Laws. Ch. 93H § 1(a).

"Data" means any material upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics. Mass. Gen Laws. Ch. 93H § 1(a).

"Encrypted" means transformation of data through the use of a 128-bit or higher algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key. Mass. Gen Laws. Ch. 93H § 1(a).

WHO MUST BE NOTIFIED?

A person or agency that maintains or stores, but does not own or license, data that includes personal information about a Massachusetts resident must notify the owner or licensor of such information when such person or agency knows or has reason to know of a breach or knows or has reason to know the personal information of such resident was acquired or used by an authorized person or used for an authorized purpose. Mass. Gen Laws. Ch. 93H § 3(a).

A person or agency that owns or licenses data that includes personal information about a Massachusetts resident must notify the following people: (1) the Attorney General; (2) the director of consumer affairs and business regulations; and (3) any affected residents when such person or agency knows or has reason to know of a breach, or knows or has reason to know the personal information of such resident was acquired or used by an authorized person or used for an authorized purpose. Such person or agency must also provide notice to any relevant consumer reporting agencies and State agencies identified and forwarded by the director of consumer affairs and business regulator to the notifying person or agency. Mass. Gen Laws. Ch. 93H § 3(b).

WHEN MUST NOTICE BE SENT?

Notice must be provided as soon as practicable, and without unreasonable delay. Mass. Gen Laws. Ch. 93H § 3(a), (b).

Notice may be delayed if a law enforcemeny agency determines that such notice may impede a criminal investigation and has notified the attorney general in writing thereof and informed the person or agency required to provide notice. As soon as the law enforcement agency determines and informs the person or agency that the required notification no longer poses a risk of impediment, notice shall be provided as soon as pracitable and without unreasonable delay. The person or agency required to provide notice must cooperative with law enforcement in its investigation. Mass. Gen Laws. Ch. 93H § 4.

IN WHAT FORM AND MANNER MUST NOTICE BE SENT?

Notice must be sent as follows:

(1) written notice;

(2) electronic notice, if notice provided is consistent with the provisions regarding electronic records and signatures set forth in § 7001(c) of Title 15 of the United States Code and chapter 110G; or

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

Substitute notice shall consist of all of the following:

(a) notice by e-mail, if the person or agency has e-mail addresses for the members of the affected class of Massachusetts residents;

(b) clear and conspicuous posting of the notice on the home page of the person or agency, if the person or agency maintains a website; and

(c) publication in, or broadcast through, media or medium that provides notice throughout the commonwealth. Mass. Gen Laws. Ch. 93H § 1(a).

WHAT MUST THE NOTICE SAY?

The notice to an *affected resident* shall include, but not be limited to:

(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 the security freeze; and

(3) any fees required to be paid to any of the consumer reporting agencies.

Notice of a breach or unauthorized acquisition or use to an *owner or licensor* of personal information by a person who maintains the personal information shall include but not be limited to:

(1) the date or approximate date of such incident;

(2) the nature of the incident; and

(3) any steps the person or agency has taken or plans to take relating to the incident.

Such notice shall not be deemed to provide notice to an affected resident. Mass. Gen Laws. Ch. 93H § 3(a).

Notice to the *attorney general*, the *director of consumer affairs and business regulation*, and *consumer reporting agencies or State agencies* shall include but not be limited to:

(1) the nature of the breach of security or unauthorized acquisiton or use;

(2) the number of Massachusetts residents affected by such incident at the time of notification; and

(3) any steps the person or agency has taken or plans to take relating to the incident.

Mass. Gen Laws. Ch. 93H § 3(a).

The notice to be provided to the attorney general and said director, and consumer reporting agencies or state agencies if any, shall include, but not be limited to: (i) the nature of the breach of security or unauthorized acquisition or use; (ii) the number of residents of the commonwealth affected by such incident at the time of notification; (iii) the name and address of the person or agency that experienced the breach of security; (iv) name and title of the person or agency reporting the breach of security, and their relationship to the person or agency that experienced the breach of security; (v) the type of person or agency reporting the breach of security; (vi) the person responsible for the breach of security, if known; (vii) the type of personal information compromised, including, but not limited to, Social Security number, driver's license number, financial account number, credit or debit card number or other data; (viii) whether the person or agency maintains a written information security program; and (ix) any steps the person or agency has taken or plans to take relating to the incident, including updating the written information security program. A person who experienced a breach of security shall file a report with the attorney general and the director of consumer affairs and business regulation certifying their credit monitoring services comply with Mass. Gen Laws. Ch. 93H § 3(a).

The notice to be provided to the resident shall include, but shall not be limited to: (i) the resident's right to obtain a police report; (ii) how a resident may request a security freeze and the necessary information to be provided when requesting the security freeze; (iii) that there shall be no charge for a security freeze; and (iv) mitigation services to be provided pursuant to this chapter; provided, however, that said notice shall not include the nature of the breach of security or unauthorized acquisition or use, or the number of residents of the commonwealth affected by said breach of security or unauthorized access or use. The person or agency that experienced the breach of security shall provide a sample copy of the notice it sent to consumers to the attorney general and the office of consumer affairs and business regulation. A notice provided pursuant to this section shall not be delayed on grounds that the total number of residents affected is not yet ascertained. In such case, and where otherwise necessary to update or correct the information required, a person or agency shall provide additional notice as soon as practicable and without unreasonable delay upon learning such additional information.

As practicable and as not to impede active investigation by the attorney general or other law enforcement agency, the office of consumer affairs and business regulation shall: (i) make available electronic copies of the sample notice sent to consumers on its website and post such notice within 1 business day upon receipt from the person that experienced a breach of security; (ii) update the breach of security notification report on its website as soon as practically possible after the information has been verified by said office but not more than 10 business days after receipt unless the information provided is not verifiable; provided, however, that the office shall

post said notice as soon as verified; (iii) amend, on a recurring basis, the breach of security notification report to include new information discovered through the investigation process or new subsequent findings from a previously reported breach of security; and (iv) instruct consumers on how they may file a public records request to obtain a copy of the notice provided to the attorney general and said director from the person who experienced a breach of security.

If the person or agency that experienced a breach of security is owned by another person or corporation, the notice to the consumer shall include the name of the parent or affiliated corporation.

If an agency is within the executive department, it shall provide written notification of the nature and circumstances of the breach of security or unauthorized acquisition or use to the executive office of technology services and security and the division of public records in the office of the state secretary as soon as practicable and without unreasonable delay following the discovery of a breach of security or unauthorized acquisition or use, and shall comply with all policies and procedures adopted by the executive office of technology services and security pertaining to the reporting and investigation of such an incident.

The department of consumer affairs and business regulation may promulgate regulations interpreting and applying this section.

Mass. Gen Laws. Ch. 93H § 3(b)-(f) (Amended by H.B. 4806).

If a person knows or has reason to know that said person experienced an incident that requires notice pursuant to section 3 and such breach of security includes a Social Security number, the person shall contract with a third party to offer to each resident whose Social Security number was disclosed in the breach of security or is reasonably believed to have been disclosed in the breach of security, credit monitoring services at no cost to said resident for a period of not less than 18 months; provided, however, that if the person that has experienced a breach of security is a consumer reporting agency, then said consumer reporting agency shall contract with a third party to offer each resident whose Social Security number was disclosed in the breach of security or is reasonably believed to have been disclosed in the breach of security, credit monitoring services at no cost to such resident for a period of not less than 42 months. Said contracts shall not include reciprocal agreements for services in lieu of payment or fees. The person or agency shall provide all information necessary for the resident to enroll in credit monitoring services and shall include information on how the resident may place a security freeze on the resident's consumer credit report.

A person that experienced a breach of security shall not require a resident to waive the resident's right to a private right of action as a condition of the offer of credit monitoring services.

The department of consumer affairs and business regulation may promulgate regulations interpreting and applying this section.

Mass. Gen Laws. Ch. 93H § 3A(a)-(c) (Amended by H.B. 4806).

ARE THERE ANY EXEMPTIONS?

A person who maintains procedures for responding to a breach of security pursuant to federal laws, rules, regulations, guidance, or guidelines is deemed to be in compliance with this chapter if the person notifies affected Massachusetts residents in accordance with the maintained or required procedures when a breach occurs; provided, further, that the person also notifies the Attorney General and the director of the office of consumer affairs and business regulation of the breach as soon as practicable and without unreasonable delay following the breach. The notice to be provided to the Attorney General and the director of the office of consumer affairs and business regulation shall consist of, but not be limited to, any steps that the person or agency has taken or plans to take relating to the breach pursuant to applicable federal law, rule, regulation, guidance or guidelines; provided, further, that if the person or agency does not comply with applicable federal laws, rules, regulations, guidance or guidelines, then it shall be subject to the provisions of the statute. Mass. Gen Laws. Ch. 93H § 5.

WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

The Attorney General may bring an action pursuant to Mass. Gen Laws. Ch. 93A § 4 against a person or otherwise to remedy violations of the statute and for other relief as may be appropriate. Mass. Gen Laws. Ch. 93H § 6.

The Attorney General may seek civil penalties of not more than $5,000 for each violation, injunctive relief, and reasonable costs and attorney's fees. Mass. Gen Laws. Ch. 93A § 4.

There is no private right of action. Mass. Gen Laws. Ch. 93A § 4.

ARE THERE ANY DATA SECURITY REQUIREMENTS IMPOSED?

Disposal of Records Containing Personal Information:

When disposing of records, each agency or person must meet the following minimum standards for proper disposal of records containing personal information:

(1) paper documents containing personal information must be either redacted, burned, pulverized or shredded so that personal data cannot practicably be read or reconstructed; and

(2) electronic media and other non-paper media containing personal information must be destroyed or erased so that personal information cannot practicably be read or reconstructed.

Any agency or person disposing of personal information may contract with a third party to dispose of personal information. Any such third party must implement and monitor compliance with policies and procedures that prohibit unauthorized access to or acquisition of or use of personal information during the collection, transportation and disposal of personal information.

Any agency or person who violates this requirement is subject to a civil fine of not more than $100 per individual affected up to a maximum of $50,000 for each instance of improper disposal.

The attorney general may file a civil action to recover these penalties. Mass. Gen Laws. Ch. 93I § 2.

Written Comprehensive Information Security Program:

Every person that owns or licenses personal information about a resident must develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards. The safeguards contained in such program must be consistent with the safeguards for protection of personal information and information of a similar character set forth in any State or federal regulations by which the person who owns or licenses such information may be regulated. Every comprehensive information security program must include, but shall not be limited to:

(1) designating one or more employees to maintain the comprehensive information security program;

(2) identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to: (a) ongoing employee training; (b) employee compliance with policies and procedures; and (c) means for detecting and preventing security system failures;

(3) developing security policies for employees relating to the storage, access and transportation of records containing personal information outside of business premises;

(4) imposing disciplinary measures for violations;

(5) preventing terminated employees from accessing records containing personal information;

(6) taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect such personal information and requiring such third-party service providers by contract to implement and maintain such appropriate security measures for personal information;

(7) reasonable restrictions upon physical access to records containing personal information, and storage of such records and data in locked facilities, storage areas or containers;

(8) regular monitoring and upgrading information safeguards as necessary to limit risks;

(9) reviewing the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the

security or integrity of records containing personal information; and

(10) documenting responsive actions taken in connection with any incident involving a breach of security, and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information.

201 Mass. Code Regs. 17.03.

Every person that owns or licenses personal information about a resident and electronically stores or transmits such information must include in its written, comprehensive information security program the establishment and maintenance of a security system covering its computers, including any wireless system, that, to the extent technically feasible, must have the following elements at a minimum:

(1) secure user authentication protocols;

(2) secure access control measures that (a) restrict access to records and files containing personal information to those who need such information to perform their job duties and (b) assign unique identifications plus passwords to each person with computer access;

(3) encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly;

(4) reasonable monitoring of systems, for unauthorized use of or access to personal information;

(5) encryption of all personal information stored on laptops or other portable devices;

(6) for files containing personal information on a system that is connected to the Internet, a reasonably up-to-date firewall protection and operating system security patches;

(7) reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be and is regularly supported with up-to-date patches and virus definitions; and

(8) education and training of employees on the proper use of the computer security system and the importance of personal information security.

201 Mass. Code Regs. 17.04.

ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

Executive Department:

If an agency is within the executive department, it shall provide written notification of the nature and circumstances of the breach or unauthorized acquisition or use to the information technology division and the division of public records as soon as practicable and without unreasonable delay following the discovery of a breach of security or unauthorized acquisition or use, and shall comply with all policies and procedures adopted by that division pertaining to the reporting and investigation of such an incident. Mass. Gen Laws. Ch. 93H § 3(c).

Consumer Reporting Agencies:

Every consumer reporting agency shall, upon request and proper identification of any consumer, clearly and accurately disclose to the consumer:

(1) the nature, contents and substance of all information, except medical information, in its file on the consumer at the time of the request, and which is obtainable based upon the identifying information supplied by the consumer when making such request, and if such consumer has made a written request, deliver a written copy, photocopy or electronic copy, of all such information except any code identifications which are used solely for purposes of transferring such information to and from consumer reporting agencies; provided, however, that the names of the users corresponding to the code identifications shall be disclosed to the consumer; and provided further, that the agency shall provide a clear, simple and plain meaning explanation of the information provided under this paragraph and such explanation shall be in a readable format and type, which shall not be smaller than 10 point type;

(2) the sources of all credit information obtained through routine credit reporting or through any other credit reporting techniques in the file at the time of the request, except that the sources of information acquired solely for use in preparing an investigative consumer report and actually used for no other purpose need not be disclosed; provided, however, that, in the event an action is brought pursuant to section 65, such sources shall be available to the plaintiff under appropriate discovery procedures in the court in which the action is brought; and

(3) the recipients of any consumer report on the consumer which it has furnished for employment purposes within the 2-year period preceding the request, and for any other purpose within the 6-month period preceding the request.

In accordance with 15 U.S.C. section 1681c-1, every consumer reporting agency, upon contact by a consumer by phone, mail or electronic communication, or in person regarding information which may be contained in the agency files regarding that consumer, shall with each written disclosure, or in response to a request by the consumer to be advised as to the consumer's rights, promptly advise the consumer of the consumer's rights under this section. The written notice shall be in a clear and conspicuous format and be no smaller than 10 point type. The notice shall

inform the consumer of the consumer's rights under this chapter, provided in a clear and conspicuous manner, in substantially the following manner:

> You have a right to obtain a copy of your credit file from a consumer credit reporting agency. You may be charged a reasonable fee not exceeding $8. There is no fee, however, if you have been turned down for credit, employment, insurance or rental dwelling because of information in your credit report within the preceding 60 days. The consumer credit reporting agency must provide someone to help you interpret the information in your credit file. Each calendar year you are entitled to receive, upon request, one free consumer credit report.
>
> You have a right to dispute inaccurate information by contacting the consumer reporting agency directly, either in writing, by mail or electronic communication through the credit reporting agency website, or by telephone. The consumer reporting agency shall provide, upon request and without unreasonable delay, a live representative of the consumer reporting agency to assist in dispute resolution whenever possible and practicable, or to the extent consistent with federal law. However, neither you nor any credit repair company or credit service organization has the right to have accurate, current and verifiable information removed from your credit report. In most cases, under state and federal law, the consumer credit reporting agency must remove accurate, negative information from your report only if it is more than 7 years old, and must remove bankruptcy information only if it is more than 10 years old.
>
> If you have notified a consumer credit reporting agency in writing that you dispute the accuracy of information in your file, the consumer credit reporting agency must then, within 30 business days, reinvestigate and modify or remove inaccurate information. The consumer credit reporting agency may not charge a fee for this service. Any pertinent information and copies of all documents you have concerning a dispute should be given to the consumer credit reporting agency.
>
> If reinvestigation does not resolve the dispute to your satisfaction, you may send a statement to the consumer credit reporting agency to keep in your file, explaining why you think the record is inaccurate. The consumer credit reporting agency must include your statement about the disputed information in a report it issues about you.
>
> You have a right to receive a record of all inquiries relating to a credit transaction initiated in the 6 months preceding your request, or 2 years in the case of a credit report used for employment purposes. This record shall include the recipients of any consumer credit report.
>
> You have the right to opt out of any prescreening lists compiled by or with the assistance of a consumer credit reporting agency by calling the agency's toll-free telephone number, or by contacting the agency through electronic communication or in writing. You may be entitled to collect compensation, in certain

circumstances, if you are damaged by a person's negligent or intentional failure to comply with the credit reporting act.

You have a right to request a "security freeze" on your consumer report. The security freeze will prohibit a consumer reporting agency from releasing any information in your consumer report without your express authorization. A security freeze shall be requested by sending a request either by toll-free telephone, secure electronic means or mail consistent with 15 U.S.C. section 1681c-1 to a consumer reporting agency. The security freeze is designed to prevent credit, loans or services from being approved in your name without your consent. You should be aware that using a security freeze may delay, interfere with, or prevent the timely approval of any subsequent request or application you make regarding new loans, credit, mortgage, insurance, government services or payments, rental housing, employment, investment, license, cellular phone, utilities, digital signature, internet credit card transactions or other services, including an extension of credit at point of sale.

When you place a security freeze on your consumer report, within 5 business days of receiving your request for a security freeze, the consumer reporting agency shall send confirmation of the security freeze consistent with 15 U.S.C. section 1681c-1.

Mass. Gen Laws. Ch. 93 §56(a), (b).

MICHIGAN

STATUTE: Mich. Comp. Laws Ann. §§ 445.61, *et seq.*,[51] 445.71, *et seq*.[52]

WHO MUST COMPLY?

A person or agency that owns, maintains or licenses data included in a database that includes personal information of a resident of Michigan. Mich. Comp. Laws Ann. § 445.72(1), (2).

An "agency" is defined as a department, board, commission, office, agency, authority, or other unit of State government, including an institution of higher education but excluding a circuit, probate, district, or municipal court. Mich. Comp. Laws Ann. § 445.63(a).

WHAT DATA IS COVERED?

The first name or first initial and last name linked to one or more of the following data elements of a Michigant resident:

(1) Social Security number;

(2) driver license number or State personal identification card number; or

(3) demand deposit or other financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to any of the resident's financial accounts.

Mich. Comp. Laws Ann. § 445.63(r).

WHAT CONSTITUTES A DATA BREACH?

Unauthorized access and acquisition of data that compromises the security or confidentiality of personal information maintained by a person or agency as part of a database of personal information regarding multiple individuals. These terms do not include unauthorized access to data by an employee or other individual if the access meets all of the following: (1) the employee or other individual acted in good faith in accessing the data; (2) the access was related to the activities of the agency or person; and (3) the employee or other individual did not misuse any personal information or disclose any personal information to an unauthorized person. Mich. Comp. Laws Ann. § 445.63(b).

[51] Publicly available at: *Identify Theft Protection Act (Excerpt)*, www.legislature.mi.gov, http://www.legislature.mi.gov/(S(mage2kx0gy2fpanhe00tqzmx))/mileg.aspx?page=GetObject&objectname=mcl-445-63 (last visited June 7, 2019).

[52] Publicly available at: *Identify Theft Protection Act (Excerpt)*, www.legislature.mi.gov, http://www.legislature.mi.gov/(S(ajsohrqidoxeeym4q11xnjto))/mileg.aspx?page=GetObject&objectname=mcl-445-71 (last visited June 7, 2019).

This statute does not apply to the access or acquisition by a person or agency of federal, State, or local government records or documents lawfully made available to the general public. Mich. Comp. Laws Ann. § 445.72(17).

Notice is not required where a resident's personal information is accessed and acquired in encrypted or redacted form unless the person gaining access also has unauthorized access to the encryption key. Mich. Comp. Laws Ann. § 445.72(1).

WHO MUST BE NOTIFIED?

A person or agency that owns or licenses data included in a database that discovers a breach (or receives notice of a breach from a person or agency that maintains the database) must notify each Michigan resident who meets one or more of the following:

(1) that resident's unencrypted and unredacted personal information was accessed and acquired by an unauthorized person; or

(2) that resident's personal information was accessed and acquired in encrypted form by a person with unauthorized access to the encryption key, unless the person or agency determines that the security breach has not or is not likely to cause substantial loss or injury to, or result in identity theft with respect to, one or more Michigan residents. In making this determination, a person or agency shall act with the care an ordinarily prudent person or agency in like position would exercise under similar circumstances. Mich. Comp. Laws Ann. § 445.72(1), (3).

A person or agency that maintains a database that includes data they not own or license that discovers a breach of the database must notify the owner or licensee of that information, unless the person or agency determines that the security breach has not or is not likely to cause substantial loss or injury to, or result in identity theft with respect to, one or more Michigan residents. In making this determination, a person or agency shall act with the care an ordinarily prudent person or agency in like position would exercise under similar circumstances. Mich. Comp. Laws Ann. § 445.72(2), (3). After a person or agency provides a notice under this section, the person or agency shall notify each consumer reporting agency that compiles and maintains files on consumers on a nationwide basis, as defined in 15 U.S.C. § 1681a(p), of the security breach without unreasonable delay. A notification under this subsection shall include the number of notices that the person or agency provided to residents of the State and the timing of those notices. Such notice is not required if either: (1) the notifying person or agency is required under this section to provide notice of a security breach to 1,000 or fewer residents; or (2) the notifying person or agency is subject to 15 U.S.C. §§ 6801 to 6809. Mich. Comp. Laws Ann. § 445.72(8).

WHEN MUST NOTICE BE SENT?

Notice should be sent without unreasonable delay, except a notifying person or agency may delay in providing notice: (1) if necessary to determine the scope of the security breach and restore the reasonable integrity of the database; or (2) when a law enforcement agency determines and advises that the required notice will impede a criminal or civil investigation or jeopardize homeland or national security. Mich. Comp. Laws Ann. § 445.72(4).

IN WHAT FORM AND MANNER MUST NOTICE BE SENT?

An agency or person shall provide any notice required under the statute by providing one or more of the following to the recipient:

(1) written notice sent to the recipient at the recipient's postal address in the records of the agency or person;

(2) written notice sent electronically to the recipient if any of the following are met:

(a) the recipient has expressly consented to receive electronic notice.

(b) the person or agency has an existing business relationship with the recipient that includes periodic e-mail communications and based on those communications the person or agency reasonably believes that it has the recipient's current e-mail address; or

(c) the person or agency conducts its business primarily through internet account transactions or on the internet.

(3) notice given by telephone by an individual who represents the person or agency if all of the following are met:

(a) the notice is not given in whole or in part by use of a recorded message; and

(b) the recipient has expressly consented to receive notice by telephone, or if the recipient has not expressly consented to receive notice by telephone, the person or agency also provides written notice if notice by telephone does not result in a live conversation within 3 business days of the initial attempt.

Mich. Comp. Laws Ann. § 445.72(5)(a)-(c).

If the person or agency demonstrates that the cost of providing notice under sections (1), (2), or (3) will exceed $250,000.00, or that the person or agency has to provide notice to more than 500,000 residents of Michigan, substitute notice may be provided by doing by doing all of the following: (A) if the person or agency has e-mail addresses for any of the residents of the State who are entitled to receive the notice, providing electronic notice to those residents; (B) if the person or agency maintains a website, conspicuously posting the notice on that website; and (C) notifying major Statewide media (such notice must include a telephone number or a website address that a person may use to obtain additional assistance and information). Mich. Comp. Laws Ann. § 445.72(5)(d).

WHAT MUST THE NOTICE SAY?

The notice must clearly communicate the following:

(1) describe the security breach in general terms;

(2) describe the type of personal information that is the subject of the unauthorized access or use;

(3) if applicable, generally describe what the agency or person providing the notice has done to protect data from further security breaches;

(4) include a telephone number where a notice recipient may obtain assistance or additional information; and

(5) remind notice recipients of the need to remain vigilant for incidents of fraud and identity theft.

Mich. Comp. Laws Ann. § 445.72(6).

ARE THERE ANY EXEMPTIONS?

A financial institution that is subject to, and has notification procedures in place that are subject to examination by the financial institution's appropriate regulator for compliance with, the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice prescribed by the Board of Governors of the Federal Reserve System and the other federal bank and thrift regulatory agencies, or similar guidance prescribed and adopted by the National Credit Union Administration and its affiliates, is considered to be in compliance with this statute. Mich. Comp. Laws Ann. § 445.72(9).

A person or agency that is subject to and complies with the Health Insurance Portability and Accountability Act ("HIPAA") of 1996, Public Law 104-191, and with regulations promulgated under that Act, 45 C.F.R. Parts 160 and 164, for the prevention of unauthorized access to customer information and customer notice, is considered to be in compliance with this statute. Mich. Comp. Laws Ann. § 445.72(10).

Effective Janurary 20, 2020, an entity that is subject to or regulated under the insurance code of 1956, 1956 PA 218, MCL 500.100 to 500.8302, is exempt from this act. Also effective January 20, 2020, an entity that owns, is owned by, or is under common ownership with an entity that is subject to or regulated under the foregoing insurance code, and maintains the same cybersecurity procedures as that other entity, is exempt from this act. Mich. Comp. Laws Ann. § 445.64(1), (2).

WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

A person that knowingly fails to provide any notice of a security breach required under the statute may be ordered to pay a civil fine of not more than $250 for each failure to provide notice. The aggregate liability of a person for multiple such violations that arise from the same security breach shall not exceed $750,000. The Attorney General or a prosecuting attorney may bring an action to recover a civil fine. Mich. Comp. Laws Ann. § 445.72(13), (14).

There is a private right of action under the statute. Mich. Comp. Laws Ann. § 445.72(15).

A person that provides notice of a security breach when a breach has not occurred, with the intent to defraud, is guilty of a misdemeanor that is punishable as follows: (a) imprisonment for not more than 93 days or a fine of not more than $250 for each violation, or both; (b) for a second violation, by imprisonment for not more than 93 days or a fine of not more than $500 for each violation, or both; and (c) for a third or subsequent violation, by imprisonment for not more than 93 days or a fine of not more than $750 for each violation, or both. Mich. Comp. Laws Ann. § 445.72(12).

ARE THERE ANY DATA SECURITY REQUIREMENTS IMPOSED?

A person or agency that maintains a database that includes personal information regarding multiple individuals must destroy any data that contains personal information concerning an individual when that data is removed from the database and the person or agency is not retaining the data elsewhere for another purpose. "Destroy" means to destroy or arrange for the destruction of data by shredding, erasing, or otherwise modifying the data so that they cannot be read, deciphered, or reconstructed through generally available means.

This does not prohibit retaining data that contain personal information for purposes of an investigation, audit, or internal review.

A person who knowingly violates this requirement is guilty of a misdemeanor and subject to a fine of not more than $250 per violation.

A person or agency is considered to be in compliance with this section if they are subject to and in compliance with federal law concerning the disposal of records containing personal identifying information. Mich. Comp. Laws Ann. § 445.72(a).

ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

A public utility that sends monthly billing or account Statements to the postal address of its customers may provide notice of a security breach to its customers in the form and manner provided above, or alternatively by providing all of the following:

(1) as applicable, written notice sent electronically in the manner provided above;

(2) notification to the media reasonably calculated to inform the customers of the public utility of the security breach;

(3) conspicuous posting of the notice of the security breach on the website of the public utility;

(4) and written notice sent in conjunction with the monthly billing or account Statement to the customer at the customer's postal address in the records of the public utility.

Mich. Comp. Laws Ann. § 445.72(11).

MINNESOTA

STATUTE: Minn. Stat. §§ 325E.61,[53] 325E.64,[54] 325M.05,[55] Minnesota Rules, part 2876.3055.[56]

WHO MUST COMPLY?

Any person or business that: (1) conducts business in Minnesota and that owns or licenses data that includes personal information; or (2) maintains data that includes personal information that the person or business does not own. Minn. Stat. § 325E.61(1)(a)-(b).

WHAT DATA IS COVERED?

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 data element is not secured by encryption or another method of technology that makes electronic data unreadable or unusable, or was secured and the encryption key, password, or other means necessary for reading or using the data was also acquired:

(1) Social Security number;

(2) driver's license number or Minnesota identification card number; or

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

Minn. Stat. § 325E.61(1)(e).

Personal information does not include publicly available information that is lawfully made available to the general public from federal, State, or local government records. Minn. Stat. § 325E.61(1)(f).

WHAT CONSTITUTES A DATA BREACH?

Any unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security system, provided that the

[53] Publicly available at: *The Office of the Revisor of Statutes*, www.revisor.mn.gov, https://www.revisor.mn.gov/statutes/?id=325E.61 (last visited June 13, 2019).
[54] Publicly available at: *The Office of the Revisor of Statutes*, www.revisor.mn.gov, https://www.revisor.mn.gov/statutes/?id=325E.64 (last visited June 13, 2019).
[55] Publicly available at: *The Office of the Revisor of Statutes*, www.revisor.mn.gov, https://www.revisor.mn.gov/statutes/cite/325M.05 (last visited June 13, 2019).
[56] Publicly available at: *The Office of the Revisor of Statutes*, https://www.revisor.mn.gov/rules/2876.3055/ (last visited June 13, 2019).

personal information is not used or subject to further unauthorized disclosure. Minn. Stat. § 325E.61(1)(d).

The statute does not apply if the data subject to the breach is encrypted or secured by another method of technology that makes electronic data unreadable or unusable, or was secured and the encryption key, password, or other means necessary for reading or using the data was also acquired. Minn. Stat. § 325E.61(1)(e).

WHO MUST BE NOTIFIED?

If the breach affects any person or business that conducts business in Minnesota and that owns or licenses data that includes personal information, that person or business must notify any Minnesota resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Minn. Stat. § 325E.61(1)(a).

If the breach affects a person or business that maintains data that includes personal information, that person or business must notify the owner or licensee of that information of the breach following discovery if personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Minn. Stat. § 325E.61(1)(b).

If a person discovers circumstances requiring notification of more than 500 persons at one time, the person shall also notify, within 48 hours, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution, and content of the notices. Minn. Stat. § 325E.61(2).

WHEN MUST NOTICE BE SENT?

Notification to an affected resident must be made in the most expedient time possible and without unreasonable delay following discovery or notification of the breach, consistent with the legitimate needs of law enforcement or with any measures necessary to determine the scope of the breach, identify the individuals affected, and restore the reasonable integrity of the data system. Minn. Stat. § 325E.61(1)(a).

Notice to the owner or licensee of affected personal information by a person or business that maintains the data must be made immediately following discovery of the breach. Minn. Stat. § 325E.61(1)(b).

A required notification may be delayed to a date certain if a law enforcement agency affirmatively determines that the notification will impede a criminal investigation. Minn. Stat. § 325E.61(1)(a).

IN WHAT FORM AND MANNER MUST NOTICE BE SENT?

Notice must be provided by one of the following methods:

(1) written notice to the most recent available address the person or business has in its records;

(2) electronic notice, if the person's primary method of communication with the individual is by electronic means, or if the notice provided is consistent with the provisions regarding electronic records and signatures in 15 U.S.C. § 7001; or

(3) substitute notice, if the person or business demonstrates that (A) the cost of providing notice would exceed $250,000, (B) that the affected class of subject persons to be notified exceeds 500,000, or (C) the person or business does not have sufficient contact information.

Substitute notice must consist of all of the following:

(1) e-mail notice when the person or business has an e-mail address for the subject persons;

(2) conspicuous posting of the notice on the website of the person or business, if the person or business maintains one; and

(3) notification to major Statewide media.

Minn. Stat. § 325E.61(1)(g).

WHAT MUST THE NOTICE SAY?

The statute does not address the contents of the notice.

ARE THERE ANY EXEMPTIONS?

This section and § 13.055(6) do not apply to any "financial institution," as defined by 15 U.S.C. § 6809(3). Minn. Stat. § 325E.61(4).

A person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of the statute and Minn. Stat. § 13.055(6) shall be deemed to be in compliance with the notification requirements of the statute and Minn. Stat. § 13.055(6) if the person or business notifies subject persons in accordance with its policies in the event of a breach. Minn. Stat. § 325E.61(1).

WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

The Attorney General has enforcement authority over the statute under Minnesota's Unfair Trade Practices statute and may seek injunctive relief and/or civil penalties up to $25,000. Minn. Stat. Ann. § 8.31.

There is no private right of action. *In re Target Corp. Data Sec. Breach Litigation*, 66 F. Supp. 3d 1154 (D. Minn. 2014) (only Minnesota Attorney General may enforce data breach statute).

ARE THERE ANY DATA SECURITY REQUIREMENTS IMPOSED?

An internet service provider, as defined under Minn. Stat. Ann. § 325M.01, must take reasonable

steps to maintain the security and privacy of personally identifiable information of any person who agrees to pay a fee to the provider for access to the internet for personal, family, or household purposes (and who does not resell access). Minn. Stat. Ann. § 325M.05; Minn. Stat. Ann. § 325M.01.

ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

Financial Institutions:

Minn. Stat. § 325E.64 provides additional requirements for financial institutions. A "financial institution" means any office of a bank, bank and trust, trust company with banking powers, savings bank, industrial loan company, savings association, credit union, or regulated lender. Minn. Stat. § 325E.64(1)(e).

No person or entity conducting business in Minnesota that accepts an access device (a card issued by a financial institution that contains a magnetic stripe, microprocessor chip, or other means for storage of information, including but not limited to, a credit card, debit card, or stored value card) in connection with a transaction shall retain the card security code data, the PIN verification code number, or the full contents of any track of magnetic stripe data, subsequent to the authorization of the transaction or in the case of a PIN debit transaction, subsequent to 48 hours after authorization of the transaction. A person or entity is in violation if its service provider retains such data. Minn. Stat. § 325E.64(2).

Whenever there is a breach of the security of the system of a person or entity that has violated Minn. Stat. § 325E.64, or that person's or entity's service provider, that person or entity shall reimburse the financial institution that issued any access devices affected by the breach for the costs of reasonable actions undertaken by the financial institution as a result of the breach in order to protect the information of its cardholders or to continue to provide services to cardholders, including but not limited to, any cost incurred in connection with:

(1) the cancellation or reissuance of any access device affected by the breach;

(2) the closure of any deposit, transaction, share draft, or other accounts affected by the breach and any action to stop payments or block transactions with respect to the accounts;

(3) the opening or reopening of any deposit, transaction, share draft, or other accounts affected by the breach;

(4) any refund or credit made to a cardholder to cover the cost of any unauthorized transaction relating to the breach; and

(5) the notification of cardholders affected by the breach.

Minn. Stat. § 325E.64(3).

The financial institution is also entitled to recover costs for damages paid by the financial institution to cardholders injured by a breach of the security of the system of a person or entity

that has violated Minn. Stat. § 325E.64. Costs do not include any amounts recovered from a credit card company by a financial institution. Minn. Stat. Ann. § 325E64.

MNvest issuers and portal operators:

Minnesota Rules, part 2876.3055, imposes additional requirements on securities issuers that offer or sell securities through "MNvest portal," as well as portal operators. MNvest issuers and portal operators must take reasonable steps to ensure that purchasers' financial and personal information is properly secured. Minn. R. 2876.3055(1)(A).

Reasonable steps include, at a minimum, a written cybersecurity policy that outlines the issuer's or portal operator's policies and procedures for: (1) preventing cybersecurity attacks that result in the disclosure, or potential disclosure, of purchasers' confidential or personally identifiable information; (2) preventing data breaches that result in the disclosure, or potential disclosure, of purchasers' confidential or personally identifiable information; (3) responding to a cybersecurity attack or data breach that occurs; and (4) demonstrating the issuer's implementation of the written cybersecurity policy. Minn. R. 2876.3055(1)(A).

The written cybersecurity policy must specifically include the MNvest issuer's or portal operator's procedures to establish compliance with Minn. Stat. Ann. § 325E.61. The cybersecurity policy must be published on the portal operator's or MNvest issuer's Web site via a prominent link on the website's homepage. Minn. R. 2876.3055(1).

In the event of a cybersecurity attack or data breach, MNvest issuers and portal operators must report to the administrator any action taken to meet the reporting requirements of Minn. Stat. § 325E.61. The report must include: (1) a general description of the type of data that were accessed or acquired; (2) the number of individuals whose data were improperly accessed or acquired; and (3) a description of the steps taken by the MNvest issuer or portal operator to notify the individuals whose data were improperly accessed or acquired. The report must be mailed or sent electronically to the administrator within 60 days of discovery of the incident. Minn. R. 2876.3055(2).

MISSISSIPPI

STATUTE: Miss. Code § 75-24-29.[57]

WHO MUST COMPLY?

Any person 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. Miss. Code § 75-24-29(1).

WHAT DATA IS COVERED?

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

(1) Social Security number;

(2) driver's license number or State identification card number; or

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

"Personal information" does not include publicly available information that is lawfully made available to the general public from federal, State, or local government records or widely distributed media. Miss. Code § 75-24-29(2)(b).

WHAT CONSTITUTES A DATA BREACH?

Unauthorized acquisition of electronic files, media, databases or computerized data containing personal information of any Mississippi resident when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable. Miss. Code § 75-24-29 (2)(a).

WHO MUST BE NOTIFIED?

Any individual who is a resident of Mississippi whose personal information was, or is reasonably believed to have been, intentionally acquired by an unauthorized person through a breach of security. Miss. Code § 75-24-29(2)(b). 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. Miss. Code. § 75-24-29(3).

If the breach affects a person that maintains computerized data which includes personal information, that person must notify the owner or licensee of that information of any breach if

[57] Publicly available at: *Mississippi Code of 1972 Unannotated*, www.lexisnexis.com, http://www.lexisnexis.com/hottopics/mscode/ (last visited June 14, 2019). Amended by S.B. 2831 to add the "Insurance Data Security Law," which was enacted on April 3, 2019 and effective July 1, 2019. Publicly available at, www.legiscan.com, https://legiscan.com/MS/text/SB2831/2019 (last visited July 19, 2019).

the personal information was, or is reasonably believed to have been, acquired by an unauthorized person for fraudulent purposes. Miss. Code § 75-24-29(4).

WHEN MUST NOTICE BE SENT?

The disclosure to affected individuals shall be made without unreasonable delay, subject to delays by law enforcement agencies and 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. Miss. Code § 75-24-29(3).

The disclosure to the owner or licensee of personal information by a person that maintains the data which includes the information must occur as soon as practicable following discovery of a breach. Miss. Code § 75-24-29(4). Any notification required may be delayed for a reasonable period of time if a law enforcement agency determines that the notification will impede a criminal investigation or national security and such agency has requested that the notification be delayed. Miss. Code. § 75-24-29(5).

IN WHAT FORM AND MANNER MUST NOTICE BE SENT?

Any notice required by the provisions of this section may be provided by one of the following methods:

(1) written notice;

(2) telephone notice;

(3) electronic notice, if the person's primary means of communication with the affected individuals is by electronic means or if the notice is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001; or

(4) substitute notice, provided the person demonstrates:

(a) that the cost of providing notice in accordance with (i), (ii), or (iii) above would exceed $5,000.000;

(b) that the affected class of subject persons to be notified exceeds 5,000 individuals; or

(c) the person does not have sufficient contact information.

Substitute notice shall consist of the following:

(1) email notice when the person has an e-mail address for the affected individuals;

(2) conspicuous posting of the notice on the website of the person if the person maintains one; and

(3) notification to major Statewide media, including newspapers, radio and television.

Miss. Code § 75-24-29(6).

WHAT MUST THE NOTICE SAY?

The statute does not address the contents of the notice.

ARE THERE ANY EXEMPTIONS?

Any person who conducts business in Mississippi that maintains its own security breach procedures as part of an information security policy for the treatment of personal information, and otherwise complies with the timing requirements of the statute, shall be deemed to be in compliance with the notification requirements of the statute if the person notifies affected individuals in accordance with the person's policies in the event of a breach of security. Any person that maintains such a security breach procedure pursuant to the rules, regulations, procedures or guidelines established by the primary or federal functional regulator, as defined in 15 U.S.C. § 6809(2), shall be deemed to be in compliance with the security breach notification requirements of the statute, provided the person notifies affected individuals in accordance with the policies or the rules, regulations, procedures or guidelines established by the primary or federal functional regulator in the event of a breach of security of the system. Miss. Code § 75-24-29(7).

WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

The State attorney general may enforce this statute. Failure to comply with the requirements of this section shall constitute an unfair trade practice. Miss. Code § 75-24-29(8). Where the violation was knowing and willful, the attorney may seek a civil penalty not to exceed $10,000 per violation. Miss. Code § 75-24-9(1)(b).

There is no private right of action. Miss. Code § 75-24-29(8).

ARE THERE ANY DATA SECURITY REQUIREMENTS IMPOSED?

No.

ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

Insurance:

"Licensee" is defined as "any person licensed, authorized to operate, or registered, or required to be licensed, authorized or registered pursuant to the insurance laws of this state, but shall not include a purchasing group or a risk-retention group chartered and licensed in a state other than this state or a person who is acting as an assuming insurer that is domiciled in another state or jurisdiction."

Each licensee shall notify the commissioner as promptly as possible but in no event later than three (3) business days from a determination that a cybersecurity event involving nonpublic information that is in the possession of a licensee has occurred when either of the following criteria has been met:

(1) this state is the licensee's state of domicile, in the case of an insurer, or this state is the licensee's home state, in the case of a producer, as those terms are defined in Section 83-17-53, and the cybersecurity event has a reasonable likelihood of materially harming a consumer residing in this state or reasonable likelihood of materially harming any material part of the normal operation(s) of the licensee; or

(2) the licensee reasonably believes that the nonpublic information involved is of two hundred fifty (250) or more consumers residing in this state and that is either of the following:

(3) a cybersecurity event impacting the licensee of which notice is required to be provided to any government body, self-regulatory agency or any other supervisory body pursuant to any state or federal law; or

(4) a cybersecurity event that has a reasonable likelihood of materially harming:

(1) any consumer residing in this state; or

(2) any material part of the normal operation(s) of the licensee.

The licensee shall provide as much of the following information as possible. The licensee shall provide the information in electronic form as directed by the commissioner. The licensee shall have a continuing obligation to update and supplement initial and subsequent notifications to the commissioner regarding material changes to previously provided information relating to the cybersecurity event:

(1) date of the cybersecurity event;

(2) description of how the information was exposed, lost, stolen or breached, including the specific roles and responsibilities of third-party service providers, if any;

(3) how the cybersecurity event was discovered;

(4) whether any lost, stolen, or breached information has been recovered and if so, how this was done;

(5) the identity of the source of the cybersecurity event;

(6) whether the licensee has filed a police report or has notified any regulatory, government or law enforcement agencies and, if so, when such notification was provided;

(7) description of the specific types of information acquired without authorization. Specific types of information means particular data elements including, for example, types of medical information, types of financial information or types of information allowing identification of the consumer;

(8) the period during which the information system was compromised by the cybersecurity event;

(9) the number of total consumers in this state affected by the cybersecurity event. The licensee shall provide the best estimate in the initial report to the commissioner and update this estimate with each subsequent report to the commissioner pursuant to this section;

(10) the results of any internal review identifying a lapse in either automated controls or internal procedures, or confirming that all automated controls or internal procedures were followed;

(11) description of efforts being undertaken to remediate the situation which permitted the cybersecurity event to occur;

(12) a copy of the licensee's privacy policy and a statement outlining the steps the licensee will take to investigate and notify consumers affected by the cybersecurity event; and

(13) name of a contact person who is both familiar with the cybersecurity event and authorized to act for the licensee.

Licensee shall comply with Section 75-24-29, as applicable, and provide a copy of the notice sent to consumers under that statute to the commissioner, when a licensee is required to notify the commissioner pursuant to the procedures above.

In the case of a cybersecurity event in a system maintained by a third-party service provider, of which the licensee has become aware, the licensee shall treat such event as it would pursuant to the procedures above unless the third-party service provider provides the notice required under pursuant to the procedures above to the commissioner.

The computation of licensee's deadlines shall begin on the day after the third-party service provider notifies the licensee of the cybersecurity event or the licensee otherwise has actual knowledge of the cybersecurity event, whichever is sooner.

Nothing in this act shall prevent or abrogate an agreement between a licensee and another licensee, a third-party service provider or any other party to fulfill any of the investigation requirements imposed under this act or notice requirements imposed under this section.

In the case of a cybersecurity event involving nonpublic information that is used by the licensee who is acting as an assuming insurer or in the possession, custody or control of a licensee who is acting as an assuming insurer and that does not have a direct contractual relationship with the affected consumers, the assuming insurer shall notify its affected ceding insurers and the commissioner of its state of domicile within 3 business days of making the determination that a cybersecurity event has occurred.

The ceding insurers that have a direct contractual relationship with affected consumers shall fulfill the consumer notification requirements imposed under Section 75-24-29 and any other notification requirements relating to a cybersecurity event imposed under this section.

In the case of a cybersecurity event involving nonpublic information that is in the possession, custody or control of a third-party service provider of a licensee who is an assuming insurer:, the assuming insurer shall notify its affected ceding insurers and the commissioner of its state of domicile within 3 business days of receiving notice from its third-party service provider that a cybersecurity event has occurred.

The ceding insurers that have a direct contractual relationship with affected consumers shall fulfill the consumer notification requirements imposed under Section 75-24-29 and any other notification requirements relating to a cybersecurity event imposed under this section.

Any licensee acting as assuming insurer shall have no other notice obligations relating to a cybersecurity event or other data breach under this section or any other law of this state.

In the case of a cybersecurity event involving nonpublic information that is in the possession, custody or control of a licensee who is an insurer or its third-party service provider for which a consumer accessed the insurer's services through an independent insurance producer, and for which consumer notice is required under Section 75-24-29, the insurer shall notify the producers of record of all affected consumers of the cybersecurity event no later than the time at which notice is provided to the affected consumers. The insurer is excused from this obligation for any producers who are not authorized by law or contract to sell, solicit or negotiate on behalf of the insurer, and in those instances in which the insurer does not have the current producer of record information for any individual consumer.

Miss. Laws 2019, S.B. 2831, § 1, *et seq.*

MISSOURI

STATUTE: Mo. Rev. Stat. § 407.1500.[58]

WHO MUST COMPLY?

Any individual, corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture, government, governmental subdivision, governmental agency, governmental instrumentality, public corporation, or any other legal or commercial entity that owns or licenses, or maintains or possesses records or data containing, personal information of residents of Missouri or any person that conducts business in Missouri that owns or licenses, or maintains or possesses records or data containing, personal information of residents of Missouri. Mo. Rev. Stat. § 407.1500(2)(1).

WHAT DATA IS COVERED?

An individual's first name or first initial and last name in combination with any one or more of the following data elements that relate to the individual if any of the data elements are not encrypted, redacted, or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable or unusable:

(1) Social Security number;

(2) driver's license number or other unique identification number created or collected by a government body;

(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 an individual's financial account;

(4) 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) medical inforrmation (any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional); or

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

Personal information does not include information that is lawfully obtained from publicly available sources, or from federal, State, or local government records lawfully made available to the general public. Mo. Rev. Stat. § 407.1500(1)(9).

[58] Publicly available at: *Revisor Of Statutes*, www.revisor.mo.gov, http://revisor.mo.gov/main/OneSection.aspx?section=407.1500&bid=23329&hl (last visited June 14, 2019).

WHAT CONSTITUTES A DATA BREACH?

Unauthorized access to and unauthorized acquisition of personal information maintained in computerized form by any individual, corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture, government, governmental subdivision, governmental agency, governmental instrumentality, public corporation, or any other legal or commercial entity that compromises the security, confidentiality, or integrity of the personal information. Good faith acquisition of personal information by a person or that person's employee or agent for a legitimate purpose of that person is not a breach of security, provided that the personal information is not used in violation of applicable law or in a manner that harms or poses an actual threat to the security, confidentiality, or integrity of the personal information. Mo. Rev. Stat. § 407.1500(1)(1).

The statute does not apply if the data subject to the breach is encrypted such that it is rendered unreadable or unusable without the use of a confidential process or key or if information is redacted, altered or truncated such that no more than 5 digits of a Social Security number or the last 4 digits of a driver's license number, State identification card number, or account number is accessible. Mo. Rev. Stat. § 407.1500(1)(9).

WHO MUST BE NOTIFIED?

Notice must be provided to any affected residents of Missouri. The owner or licensee of the information must also be notified if the breach affects a third-party who maintains data on behalf of a covered entity. Mo. Rev. Stat. § 407.1500(2)(1)-(2).

In the event that the breached entity notifies more than 1,000 consumers at one time, it shall notify, without unreasonable delay, the State Attorney General's office and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution, and content of the notice. Mo. Rev. Stat. § 407.1500(2)(8).

Notice is not required if, after an appropriate investigation by the breached entity or after consultation with the relevant federal, State, or local agencies responsible for law enforcement, the person determines that a risk of identity theft or other fraud to any individual resident is not reasonably likely to occur as a result of the breach. Such a determination shall be documented in writing and the maintained for 5 years. Mo. Rev. Stat. § 407.1500(2)(5).

WHEN MUST NOTICE BE SENT?

Notice to an affected resident must be made without unreasonable delay, consistent with the legitimate needs of law enforcement and with any measures necessary to determine sufficient contact information and to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system. Mo. Rev. Stat. § 407.1500(2)(1).

Notice to the owner or licensee of affected information by a person or business that maintains the data must be made immediately following discovery of the breach, consistent with the legitimate needs of law enforcement. Mo. Rev. Stat. § 407.1500(2)(2).

Notice may be delayed if a law enforcement agency informs the person that notification may impede a criminal investigation or jeopardize national or homeland security, provided that such request by law enforcement is made in writing or the person documents such request contemporaneously in writing. Notice shall be provided without unreasonable delay after the agency communicates to the person its determination that notice will no longer impede the investigation or jeopardize national or homeland security. Mo. Rev. Stat. § 407.1500(2)(3).

IN WHAT FORM AND MANNER MUST NOTICE BE SENT?

Notice to affected residents shall be provided by one of the following methods:

(1) written notice;

(2) electronic notice for those consumers for whom the person has a valid E-mail address and who have agreed to receive communications electronically, if the notice provided is consistent with the provisions of 15 U.S.C. § 7001 regarding electronic records and signatures for notices legally required to be in writing;

(3) telephonic notice, if such contact is made directly with the affected consumers; or

(4) substitute notice, if:

(a) the person demonstrates that the cost of providing notice would exceed $100,000;

(b) the class of affected consumers to be notified exceeds 150,000;

(c) the person does not have sufficient contact information or consent to satisfy paragraphs (1), (2), or (3), for only those affected consumers without sufficient contact information or consent; or

(d) the person is unable to identify particular affected consumers, and only for those unidentifiable consumers.

Mo. Rev. Stat. § 407.1500(2)(6).

Substitute notice shall consist of all the following:

(1) e-mail notice when the person has an e-mail address for the affected consumer;

(2) conspicuous posting of the notice or a link to the notice on the website of the person if the person maintains one; and

(3) notification to major Statewide media. Mo. Rev. Stat. § 407.1500(2)(7).

WHAT MUST THE NOTICE SAY?

The notice must at minimum include a description of the following:

(1) the incident in general terms;

(2) the type of personal information that was obtained as a result of the breach of security;

(3) a telephone number that the affected consumer may call for further information and assistance, if one exists;

(4) contact information for consumer reporting agencies; and

(5) advice that directs the affected consumer to remain vigilant by reviewing account Statements and monitoring free credit reports.

Mo. Rev. Stat. § 407.1500(2)(4).

ARE THERE ANY EXEMPTIONS?

A financial institution shall be deemed to be in compliance with this section if it is:

(1) subject to and in compliance with the Federal Interagency Guidance Response Programs for Unauthorized Access to Customer Information and Customer Notice, issued on March 29, 2005, by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision, and any revisions, additions, or substitutions relating thereto;

(2) subject to and in compliance with the National Credit Union Administration regulations in 12 C.F.R. Part 748; or

(3) subject to and in compliance with the provisions of Title V of the Gramm-Leach-Bliley Financial Modernization Act of 1999.

Mo. Rev. Stat. § 407.1500(3)(3).

A person that maintains its own notice procedures as part of an information security policy for the treatment of personal information, and whose procedures are otherwise consistent with the timing requirements of the statute, is deemed to be in compliance with the notice requirements if the person notifies affected consumers in accordance with its policies in the event of a security breach. Mo. Rev. Stat. § 407.1500(3)(1).

A person that is regulated by State or federal law and that maintains procedures for a security breach pursuant to the laws, rules, regulations, guidances, or guidelines established by its primary or functional State or federal regulator is deemed to be in compliance with the statute if the person notifies affected consumers in accordance with the maintained procedures when a breach occurs. Mo. Rev. Stat. § 407.1500(3)(2).

Back to TOC

WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

The Attorney General shall have exclusive authority to bring an action to obtain actual damages for a willful and knowing violation of this section. The Attorney General may seek a civil penalty not to exceed $150,000 per breach or series of breaches of a similar nature that are discovered in a single investigation. Mo. Rev. Stat. § 407.1500(4).

ARE THERE ANY DATA SECURITY REQUIREMENTS IMPOSED?

No.

ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

None.

MONTANA

STATUTE: Mont. Code Ann. **§§** 2-6-1501 – 2-6-1503,[59] 30-14-1701 *et seq.*,[60] and 33-19-321.[61]

WHO MUST COMPLY?

Any person or business that: (1) conducts business in Montana and that owns or licenses computerized data that includes personal information; or (2) maintains computerized data that includes personal information. Mont. Code § 30-14-1704(1), (2).

Any State agency that maintains computerized data containing personal information. Mont. Code Ann. § 2-6-1503(1).

WHAT DATA IS COVERED?

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 data elements are not encrypted:

(1) a Social Security number;

(2) driver's license, State identification card, or tribal identification card number;

(3) an account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to a person's financial account;

(4) medical record information, meaning information relates to an individual's physical or mental condition, medical history, medical claims history, or medical treatment or is obtained from a medical professional or medical care institution, from the individual, or from the individual's spouse, parent, or legal guardian (*see* Mont. Code Ann. § 33-19-104);

(5) a taxpayer identification number; or

(6) an identity protection personal identification number issued by the I.R.S.

The term does not include publicly available information that is lawfully made available from federal, State, local, or tribal government records. Mont. Code Ann. § 30-14-1704(4)(b)(ii).

---

[59] Publicly available at: *Montana Code Annotated 2017*, www.leg.mt.gov, https://leg.mt.gov/bills/mca/title_0020/chapter_0060/part_0150/sections_index.html (last visited June 22, 2019).
[60] Publicly available at: *Montana Code Annotated 2017*, www.leg.mt.gov, https://leg.mt.gov/bills/mca/title_0300/chapter_0140/part_0170/sections_index.html (last visited June 22, 2019).
[61] Publicly available at: *Montana Code Annotated 2017*, www.leg.mt.gov, https://leg.mt.gov/bills/mca/title_0330/chapter_0190/part_0030/section_0210/0330-0190-0030-0210.html (last visited June 22, 2019).

WHAT CONSTITUTES A DATA BREACH?

Unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the person or business and causes or is reasonably believed to cause loss or injury to a Montana resident. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the data system, provided that the personal information is not used or subject to further unauthorized disclosure. Mont. Code Ann. § 30-14-1704(4)(a).

The statute does not apply if the data subject to the breach is encrypted. The statute does not define encryption. Mont. Code Ann. § 30-14-1704(4)(b)(i).

WHO MUST BE NOTIFIED?

A resident of Montana whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. Mont. Code Ann. § 30-14-1704(1).

If the breach affects a person or business that maintains covered personal information, that person must notify the owner or licensee of that information if the personal information was or is reasonably believed to have been acquired by an unauthorized person. Mont. Code Ann. § 30-14-1704(2).

If a business gives notice of a breach to an individual that suggests, indicates, or implies that the individual may obtain a copy of their file from a consumer credit reporting agency, the business must coordinate with the consumer reporting agency as to the timing, content, and distribution of the notice to the individual. This may not unreasonably delay any required notice to affected individuals. Mont. Code § 30-14-1704(7).

Any person or business that is required to issue a notification shall simultaneously submit an electronic copy of the notification and a Statement providing the date and method of distribution of the notification to the 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, a single copy of the notification must be submitted that indicates the number of individuals in Montana who received notification. Mont. Code Ann. § 30-14-1704(8).

WHEN MUST NOTICE BE SENT?

Notification to affected residents must be made without unreasonable delay, consistent with the legitimate needs of law enforcement or with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. Mont. Code § 30-14-1704(1).

Notification to the owner or licensee of affected personal information by a person or business that maintains the data must be made immediately following discovery of the breach. Mont. Code § 30-14-1704(2).

The required notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation and requests a delay in notification. The required notification must be made after the agency determines that it will not compromise the investigation. Mont. Code § 30-14-1704(3).

IN WHAT FORM AND MANNER MUST NOTICE BE SENT?

Notice must be provided by one of the following methods:

(1) written notice;

(2) electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001;

(3) telephonic notice; or

(4) substitute notice, if the notifying person or business demonstrates that:

(a) the cost of providing notice would exceed $250,000;

(b) the affected class of subject persons to be notified exceeds 500,000; or

(c) the person or business does not have sufficient contact information.

Substitute notice must consist of the following:

(1) an e-mail notice when the person or business has an e-mail address for the subject persons and conspicuous posting of the notice on the website page of the person or business if the person or business maintains one; or

(2) notification to applicable local or Statewide media.

Mont. Code Ann. § 30-14-1704(5).

WHAT MUST THE NOTICE SAY?

The statute does not address the contents of the notice.

ARE THERE ANY EXEMPTIONS?

A person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and that does not unreasonably delay notice is considered to be in compliance with the notification requirements of the statute if the person or business notifies subject persons in accordance with its policies in the event of a security breach. Mont. Code Ann. § 30-14-1704(6).

WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

Whenever the Montana Department of Justice has reason to believe that a person has violated the statute and that proceeding would be in the public interest, the Department may bring an action in against the person for injunctive relief or a temporary restraining order upon provision of the notice required under § 30-14-111(2). Mont. Code Ann. § 30-14-1705(1).

A violation of this statute shall constitute an unfair method of competition and unfair or deceptive act or practice and is subject to the penalties set forth in § 30-14-142. Mont. Code Ann. § 30-14-1705(3).

A person who engages in a willful violation may face a civil fine of not more than $10,000 per violation. A person who engages in a fraudulent course of conduct may be imprisoned for not more than 1 year, fined in an amount not more than $5,000, or both. Mont. Code Ann. § 30-14-142.

ARE THERE ANY DATA SECURITY REQUIREMENTS IMPOSED?

A business shall take all reasonable steps to destroy or arrange for the destruction of a customer's records within its custody or control containing personal information that is no longer necessary to be retained by the business by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable or undecipherable. Mont. Code Ann. § 30-14-1703.

ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

Insurance:

Section 33-19-321 adds the following requirements for any licensee or insurance-support organization that conducts business in Montana.

Any person to whom personal information is disclosed in order for the person to perform an insurance function pursuant to § 33–19–301, *et seq*., that maintains computerized data that includes personal information shall notify the licensee or insurance-support organization of any breach of the security of the system in which the data is maintained immediately following discovery of the breach if the personal information was or is reasonably believed to have been acquired by an unauthorized person. Mont. Code Ann. § 33-19-321(2).

Licensees, insurance-support organizations, and persons to whom personal information is disclosed pursuant to § 33–19–301, *et seq.*, shall develop and maintain an information security policy for the safeguarding of personal information and security breach notice procedures that provide expedient notice to individuals. Mont. Code Ann. § 33-19-321(4).

Any licensee or insurance-support organization that is required to issue a notification pursuant to this section shall simultaneously submit an electronic copy of the notification and a Statement providing the date and method of distribution of the notification to the Montana insurance commissioner, excluding any information that personally identifies any individual who is entitled to receive notification. If a notification is made to more than one individual, a single copy of the

notification must be submitted that indicates the number of individuals in the State who received notification. Mont. Code Ann. § 33-19-321(5).

State Agencies:

Upon discovery or notification of a breach of the security of a data system, a State agency that maintains computerized data containing personal information in the data system shall make reasonable efforts to notify any person whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. Mont. Code Ann. § 2-6-1503(1).

A third-party that receives personal information from a State agency and maintains that information in a computerized data system to perform a State agency function shall:

(1) notify the State agency immediately following discovery of the breach if the personal information is reasonably believed to have been acquired by an unauthorized person; and

(2) make reasonable efforts upon discovery or notification of a breach to notify any person whose unencrypted personal information is reasonably believed to have been acquired by an unauthorized person as part of the breach. This notification must be provided in the same manner as the notification required in subsection (1).

Mont. Code Ann. § 2-6-1503(2)(a).

A State agency notified of a breach by a third-party has no independent duty to provide notification of the breach if the third-party has provided such notification in the manner required but must provide notification if the third-party fails to do so in a reasonable time and may recover its reasonable costs from the third-party. Mont. Code Ann. § 2-6-1503(2)(a).

All State agencies and third-parties to whom personal information is disclosed by a State agency shall develop and maintain:

(1) an information security policy designed to safeguard personal information; and

(2) breach notification procedures that provide reasonable notice to individuals.

Mont. Code Ann. § 2-6-1503(4).

A State agency or third-party that is required to issue a notification to an affected individual shall simultaneously submit to the State's chief information officer at the department of administration and to the attorney general's consumer protection office an electronic copy of the notification and a Statement providing the date and method of distribution of the notification. The electronic copy and Statement of notification must exclude any information that identifies the person who is entitled to receive notification. If notification is made to more than one individual, a single copy of the notification that includes the number of people notified must be submitted to the chief information officer and the consumer protection office. Mont. Code Ann. § 2-6-1503(5).

NEBRASKA

STATUTE: Neb. Rev. Stat. §§ 87-801 to 807.[62]

WHO MUST COMPLY?

An individual or a commercial entity that: (1) conducts business in Nebraska and that owns or licenses computerized data that includes personal information about about a Nebraska resident; or (2) maintains computerized data that includes personal information about a Nebraska resident. Neb. Rev. Stat. § 87-803(1), (2).

"Commercial entity" includes any corporation, business trust, eState, trust, partnership, limited partnership, limited liability partnership, limited liability company, association, organization, joint venture, government, governmental subdivision, agency, or instrumentality, or any other legal entity, whether for profit or not for profit. Neb. Rev. Stat. § 87-802(2).

WHAT DATA IS COVERED?

A Nebraska resident's first name or first initial and last name in combination with any one or more of the following data elements that relate to the resident if either the name or the data elements are not encrypted, redacted, or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable:

(1) Social Security number;

(2) motor vehicle operator's license number or State identification card number;

(3) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial account;

(4) unique electronic identification number or routing code, in combination with any required security code, access code, or password;

(5) unique biometric data, such as a fingerprint, voice print, or retina or iris image, or other unique physical representation; or

(6) a user name or e-mail address, in combination with a password or security question and answer, that would permit access to an online account.

Personal information does not include publicly available information that is lawfully made available to the general public from federal, State, or local government records. Neb. Rev. Stat. § 87-802(5).

[62] Publicly available at: *Nebraska Legislature*, www.nebraskalegislature.gov, http://nebraskalegislature.gov/laws/statutes.php?statute=87-801 (last visited June 22, 2019).

WHAT CONSTITUTES A DATA BREACH?

Unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an individual or a commercial entity. Neb. Rev. Stat. § 87-802(1).

Good faith acquisition of personal information by an employee or agent of an individual or a commercial entity for the purposes of the individual or the commercial entity is not a breach of the security of the system if the personal information is not used or subject to further unauthorized disclosure. Acquisition of personal information pursuant to a search warrant, subpoena, or other court order or pursuant to a subpoena or order of a State agency is not a breach of the security of the system. Neb. Rev. Stat. § 87-802(1).

Data shall not be considered encrypted if the confidential process or key was or is reasonably believed to have been acquired as a result of the breach of the security of the system. Neb. Rev. Stat. § 87-802(3).

WHO MUST BE NOTIFIED?

The affected Nebraska resident and, not later than the time when notice is provided to a Nebraska resident, the State attorney general, if a good-faith, reasonable, and prompt investigation determines that the use of information about a Nebraska resident for an unauthorized purpose has occurred or is reasonably likely to occur. Neb. Rev. Stat. § 87-803(1)-(2).

If the breach affects an individual or commercial entity that maintains covered information, the owner or licensee of that information, if use of personal information about a Nebraska resident for an unauthorized purpose occurred or is reasonably likely to occur. Neb. Rev. Stat. § 87-803(3).

WHEN MUST NOTICE BE SENT?

Notice to affected residents and the attorney general must be made as soon as 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. Neb. Rev. Stat. § 87-803(4).

Notice to owners or licensees of personal information must be made by the individual or community that maintains the personal information when it becomes aware of a breach. Neb. Rev. Stat. § 87-803(3).

Notice may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation. Notice shall be made in good faith, without unreasonable delay, and as soon as possible after the law enforcement agency determines that notification will no longer impede the investigation. Neb. Rev. Stat. § 87-803(4).

IN WHAT FORM AND MANNER MUST NOTICE BE SENT?

Notice must be sent in the following manner:

(1) written notice;

(2) telephonic notice;

(3) electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001, as such section existed on January 1, 2006; or

(4) substitute notice, if the individual or commercial entity required to provide notice demonstrates:

(a) that the cost of providing notice will exceed 75,000;

(b) that the affected class of Nebraska residents to be notified exceeds 100,000 residents; or

(c) that the individual or commercial entity does not have sufficient contact information to provide notice.

Neb. Rev. Stat. § 87-802(4)(a)-(c).

Substitute notice under this subdivision requires all of the following:

(1) e-mail notice if the individual or commercial entity has e-mail addresses for the members of the affected class of Nebraska residents,

(2) conspicuous posting of the notice on the web site of the individual or commercial entity if the individual or commercial entity maintains a web site, and

(3) notice to major Statewide media outlets.

Neb. Rev. Stat. § 87-802(4)(d).

If the individual or commercial entity required to provide notice has 10 or less employees and demonstrates that the cost of providing notice will exceed $10,000, then substitute notice requires all of the following:

(1) e-mail notice if the individual or commercial entity has e-mail addresses for the members of the affected class of Nebraska residents;

(2) notification by a paid advertisement in a local newspaper that is distributed in the geographic area in which the individual or commercial entity is located, which advertisement shall be of sufficient size that it covers at least one-quarter of a page in the newspaper and shall be published in the newspaper at least once a week for three consecutive weeks;

(3) conspicuous posting of the notice on the web site of the individual or commercial entity if the individual or commercial entity maintains a web site; and

(4) notification to major media outlets in the geographic area in which the individual or commercial entity is located.

Neb. Rev. Stat. § 87-802(4)(e).

WHAT MUST THE NOTICE SAY?

The statute does not address the contents of the notice.

ARE THERE ANY EXEMPTIONS?

An individual or a commercial entity that maintains its own notice procedures which are part of an information security policy for the treatment of personal information and which are otherwise consistent with the timing requirements of § 87-803, is deemed to be in compliance with the notice requirements of § 87-803 if the individual or the commercial entity notifies affected Nebraska residents and the Attorney General in accordance with its notice procedures in the event of a breach of the security of the system. Neb. Rev. Stat. § 87-804(1).

An individual or a commercial entity that is regulated by State or federal law and that maintains procedures for a breach of the security of the system pursuant to the laws, rules, regulations, guidance, or guidelines established by its primary or functional State or federal regulator is deemed to be in compliance with § 87-803 if the individual or commercial entity notifies affected Nebraska residents and the Attorney General in accordance with the maintained procedures in the event of a breach of the security of the system. Neb. Rev. Stat. § 87-804(2).

WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

The Attorney General may issue subpoenas and seek and recover direct economic damages for each affected Nebraska resident injured by a violation of the statute. Neb. Rev. Stat. § 87-806(1).

A violation of § 87-808 shall be considered a violation of § 59-1602, which deems any unfair method of competition and unfair or deceptive act or practice in the conduct of any trade or commerce to be unlawful. No private right of action exists for a violation of § 87-808. Neb. Rev. Stat. § 87-806(2).

ARE THERE ANY DATA SECURITY REQUIREMENTS IMPOSED?

An individual or a commercial entity that conducts business in Nebraska and owns, licenses, or maintains computerized data that includes personal information about a Nebraska resident must implement and maintain reasonable security procedures and practices that are appropriate to the nature and sensitivity of the personal information owned, licensed, or maintained and the nature and size of, and the resources available to, the business and its operations, including safeguards that protect the personal information when the individual or commercial entity disposes of the personal information. Neb. Rev. Stat. § 87-808(1).

For any contract entered or renewed on or after July 19, 2018, an individual or commercial entity that discloses computerized data that includes personal information about a Nebraska resident to a nonaffiliated, third-party service provider must require by contract that the service provider implement and maintain reasonable security procedures and practices that are: (1) appropriate to the nature of the personal information disclosed to the service provider; and (2 reasonably designed to help protect the personal information from unauthorized access, acquisition, destruction, use, modification, or disclosure. Neb. Rev. Stat. § 87-808(2).

An individual or a commercial entity complies with the reasonable security procedures and practices requirements of § 87-808 if the individual or commercial entity complies with: (1) a State or federal law that provides greater protection to personal information than the protections provided by § 87-808; or (2) the regulations promulgated under Title V of the Gramm-Leach-Bliley Act, or the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as such acts and sections existed on January 1, 2018, if the individual or commercial entity is subject to either or both of such acts or sections. Neb. Rev. Stat. Ann. § 87-808(3).

ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

None.

NEVADA

STATUTE: Nev. Rev. Stat. §§ 603A.010 – 603A.290,[63] 242.181,[64] 242.183,[65] 439.591.[66]

WHO MUST COMPLY?

Any data collector that owns, maintains, or licenses computerized data which includes personal information. Nev. Rev. Stat. § 603A.220(1)-(2).

"Data collector" means any governmental agency, institution of higher education, corporation, financial institution or retail operator or any other type of business entity or association that, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates or otherwise deals with nonpublic personal information. Nev. Rev. Stat. § 603A.030.

WHAT DATA IS COVERED?

A natural person'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 data elements are not encrypted:

(1) Social Security number;

(2) driver's license number, driver authorization card number or 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 the person's financial account;

(4) a medical identification number or a health insurance identification number; or

(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.

Nev. Rev. Stat. § 603A.040(1).

The following data is not covered: (1) the last four digits of a Social Security number, a driver's license number, a driver authorization card number, or an identification card number; or (2) publicly available information that is lawfully made available to the general public from federal, State or local governmental records. Nev. Rev. Stat. § 603A.040(2).

---

[63] Publicly available at: *Security of Personal Information*, www.leg.State.nv.us, http://www.leg.State.nv.us/NRS/NRS-603A.html (last visited June 23, 2019).
[64] Publicly available at: *Information Services*, www.leg.State.nv.us, http://www.leg.State.nv.us/NRS/NRS-242.html#NRS242Sec181 (last visited June 23, 2019).
[65] Publicly available at: *Information Services*, www.leg.State.nv.us, http://www.leg.State.nv.us/NRS/NRS-242.html#NRS242Sec183 (last visited June 23, 2019).
[66] Publicly available at: *Information Services*, www.leg.State.nv.us, https://www.leg.State.nv.us/NRS/NRS-439.html (last visited June 23, 2019).

WHAT CONSTITUTES A DATA BREACH?

The unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information maintained by the data collector. This does not include the good faith acquisition of personal information by an employee or agent of the data collector for a legitimate purpose of the data collector, so long as the personal information is not used for a purpose unrelated to the data collector or subject to further unauthorized disclosure. Nev. Rev. Stat. § 603A.020.

The statute does not apply if the data subject to the breach is encrypted. The statute does not define encryption. Nev. Rev. Stat. § 603A.040(1).

WHO MUST BE NOTIFIED?

Any resident of this State whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Nev. Rev. Stat. § 603A.220(1).

If the breach affects a data collector that maintains personal information, the data collector must notify the owner or licensee of the information of the breach if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Nev. Rev. Stat. § 603A.220(2).

If a data collector determines that notification is required to be given to more than 1,000 persons at any one time, the data collector shall also notify, without unreasonable delay, any consumer reporting agency that compiles and maintains files on consumers on a nationwide basis, of the time the notification is distributed and the content of the notification. Nev. Rev. Stat. § 603A.220(6).

WHEN MUST NOTICE BE SENT?

Disclosure to affected residents 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 system data. Nev. Rev. Stat. § 603A.220(1).

Disclosure to the owner or licensee of personal information by a person that maintains the data which includes the information must be made immediately following discovery of the breach. Nev. Rev. Stat. § 603A.220(2).

Notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section must be made after the law enforcement agency determines that the notification will not compromise the investigation. Nev. Rev. Stat. § 603A.220(3).

IN WHAT FORM AND MANNER MUST NOTICE BE SENT?

Notification required by this section must be provided by one of the following methods:

(1) written notification;

electronic notification, if the notification provided is consistent with the provisions of the Electronic Signatures in Global and National Commerce Act, 15 U.S.C. §§ 7001 *et seq.*; or

substitute notification, if the data collector demonstrates:

(1) that the cost of providing notification would exceed $250,000;

(2) the affected class of subject persons to be notified exceeds 500,000; or

(3) the data collector does not have sufficient contact information.

Nev. Rev. Stat. § 603A.220(4)(c).

Substitute notification must consist of all the following:

(1) notification by e-mail when the data collector has e-mail addresses for the subject persons,

(2) conspicuous posting of the notification on the website of the data collector, if the data collector maintains a website, and

(3) notification to major Statewide media.

Nev. Rev. Stat. § 603A.220(4).

WHAT MUST THE NOTICE SAY?

The statute does not address the contents of the notification.

ARE THERE ANY EXEMPTIONS?

A data collector which satisfies either of the following will be deemed to be in compliance with the notification requirements of the statute:

(2) maintains its own notification policies and procedures as part of an information security policy for the treatment of personal information that is otherwise consistent with the timing requirements of the statute if the data collector notifies subject persons in accordance with its policies and procedures in the event of a breach; or

(3) is subject to and complies with the privacy and security provisions of the Gramm-Leach-Bliley Act.

Nev. Rev. Stat. § 603A.220(5).

The statute does not apply to the maintenance or transmittal of electronic health records in accordance with Nev. Rev. Stat. §§ 439.581-595; Nev. Rev. Stat. § 603A.100.

WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

If the Attorney General or a district attorney of any county has reason to believe that any person is violating, proposes to violate, or has violated the provisions of the statute, the Attorney General or district attorney may bring an action against that person for temporary or permanent injunctive relief. Nev. Rev. Stat. § 603A.290.

A data collector that provides the required notification may commence an action for damages against a person that unlawfully obtained or benefited from personal information obtained from records maintained by the data collector. A data collector that prevails in such an action may be awarded damages which may include, without limitation, the reasonable costs of notification, reasonable attorney's fees and costs, and punitive damages. The costs of notification include, without limitation, labor, materials, postage and any other costs reasonably related to providing the notification. Nev. Rev. Stat. § 603A.270.

A court may order a person who is convicted of unlawfully obtaining or benefiting from personal information obtained as a result of such breach to pay restitution to the data collector for the reasonable costs incurred by the data collector in providing the required notification, including, without limitation, labor, materials, postage and any other costs reasonably related to providing such notification. Nev. Rev. Stat. § 603A.280.

ARE THERE ANY DATA SECURITY REQUIREMENTS IMPOSED?

A business that maintains records which contain personal information concerning the customers of the business shall take reasonable measures to ensure the destruction of those records when the business decides that it will no longer maintain the records. "Reasonable measures to ensure the destruction" means any method that modifies the records containing the personal information in such a way as to render the personal information contained in the records unreadable or undecipherable, including, without limitation: (1) shredding of the record containing the personal information; or (2) erasing of the personal information from the record. Nev. Rev. Stat. Ann. § 603A.200.

A data collector that maintains records which contain personal information of a Nebraska resident, or any person with whom a data collector contracts for the disclosure of the personal information of a Nebraska resident, must implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure. Nev. Rev. Stat. Ann. § 603A.210(1)-(2).

A data collector doing business in Nevada who does not accept a payment card in connection with a sale of goods or services may not:

(1) transfer any personal information through an electronic, non-voice transmission other than a facsimile to a person outside of the secure system of the data

collector unless the data collector uses encryption to ensure the security of electronic transmission; or

(2) move any data storage device containing personal information beyond the logical or physical controls of the data collector, its data storage contractor or, if the data storage device is used by or is a component of a multifunctional device, a person who assumes the obligation of the data collector to protect personal information, unless the data collector uses encryption to ensure the security of the information.

Nev. Rev. Stat. Ann. § 603A.215(2).

ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

State Agency or Elected State Officer:

Any State agency or elected State officer which uses the equipment or services of the Division of Enterprise Information Technology Services within the Department of Administration must report to the Office of Information Security of the Division any suspected incident of:

(1) unauthorized access to an information system or application of an information system of the Division used by the State agency or elected State officer; and

(2) noncompliance with the regulations, standards, practices, policies and conventions of the Division that is identified by the Division as security-related, within 24 hours after discovery of the suspected incident. If the Office determines that an incident of unauthorized access or noncompliance occurred, the Office must immediately report the incident to the Administrator of the Division. Nev. Rev. Stat. Ann. § 242.181.

The Administrator of the Division or Chief of the Office of Information Security may, in their discretion, inform members of the Technological Crime Advisory Board, the Nevada Commission on Homeland Security, and the Information Technology Advisory Board of any: (1) breach of an information system of a State agency or elected officer or application of such an information system; or (2) unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of such an information system. Nev. Rev. Stat. § 242.183(2).

Electronic Health Records:

Nev. Rev. Stat. §§ 439.581 to 439.595 sets forth specific requirements for electronic health records, including but not limited to the requirement that a patient be notified if the confidentiality of information contained in an electronic health record of the patient is breached. Nev. Rev. Stat. § 439.591(2).

Acceptance of Payment Card:

If a data collector doing business in this State accepts a payment card in connection with a sale of goods or services, the data collector must comply with the current version of the Payment Card

Industry (PCI) Data Security Standard, as adopted by the PCI Security Standards Council or its successor organization, with respect to those transactions, not later than the date for compliance set forth in the PCI Data Security Standard or by the PCI Security Standards Council or its successor organization. Nev. Rev. Stat. § 603A.215.

NEW HAMPSHIRE

STATUTE: N.H. Rev. Stat. §§ 189:65 – 189:68-a,[67] 332-I:1 et seq.,[68] 359-C:19,[69] 359-C:20,[70] and 359-C:21.[71]

WHO MUST COMPLY?

Any person doing business in New Hampshire who owns or licenses computerized data that includes personal information. Any person or business that maintains computerized data that includes personal information. N.H. Rev. Stat. § 359-C:20(I).

"Person" is an individual, corporation, trust, partnership, incorporated or unincorporated association, limited liability company, or other form of entity, or any agency, authority, board, court, department, division, commission, institution, bureau, or other State governmental entity, or any political subdivision of the State. N.H. Rev. Stat. § 359-C:19(III).

WHAT DATA IS COVERED?

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

(1) Social Security number;

(2) driver's license number or other government identification number; or

(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.

Personal information does not include information that is lawfully made available to the general public from federal, State, or local government records. N.H. Rev. Stat. § 359-C:19(IV).

---

[67] Publicly available at: *Student and Teacher Information Protection and Privacy, www.gencourt.State.nh.us,* http://www.gencourt.State.nh.us/rsa/html/XV/189/189-65.htm (last visited July 19, 2019). This statute was amended by H.B.1612, approved June 12, 2018 and with an effective date of August 11, 2018, which requires the State's Department of Education to establish minimum standards for maintaining the privacy and security of student and employee data for local education agencies and requires each local education agency to develop a data and privacy governance plan with certain enumerated elements. The bill is publicly available at: https://legiscan.com/NH/text/HB1612/2018 (last visited July 19, 2019).

[68] Publicly available at: *Medical Records, Patient Information, and the Health Information Organization Corporation, www.gencourt.State.nh.us,* http://www.gencourt.State.nh.us/rsa/html/xxx/332-i/332-I-1.htm (last visited July 19, 2019).

[69] Publicly available at: *Notice of Security Breach,* www.gencourt.State.nh.us, http://www.gencourt.State.nh.us/rsa/html/XXXI/359-C/359-C-19.htm (last visited July 19, 2019).

[70] Publicly available at: *Notice of Security Breach,* www.gencourt.State.nh.us, http://www.gencourt.State.nh.us/rsa/html/XXXI/359-C/359-C-20.htm (last visited July 19, 2019).

[71] Publicly available at: *Notice of Security Breach,* www.gencourt.State.nh.us, http://www.gencourt.State.nh.us/rsa/html/XXXI/359-C/359-C-21.htm (last visited July 19, 2019).

WHAT CONSTITUTES A DATA BREACH?

The unauthorized acquisition of computerized data that compromises the security or confidentiality of personal information maintained by a person doing business in the State. Good faith acquisition of personal information by an employee or agent of a person for the purposes of the person's business shall not be considered a security breach, provided that the personal information is not used or subject to further unauthorized disclosure. N.H. Rev. Stat. § 359-C:19(V).

The statute does not apply if the data subject to the breach is encrypted. "Encrypted" means the transformation of data through the use of an algorithmic process into a form for which there is a low probability of assigning meaning without use of a confidential process or key, or securing the information by another method that renders the data elements completely unreadable or unusable. Data shall not be considered to be encrypted if it is acquired in combination with any required key, security code, access code, or password that would permit access to the encrypted data. N.H. Rev. Stat. § 359-C:19(II).

WHO MUST BE NOTIFIED?

Any affected individuals, if it is determined that misuse of personal information has occurred or is reasonably likely to occur, or if a determination cannot be made. N.H. Rev. Stat. § 359-C:20(I)(a).

Any person engaged in trade or commerce that is subject to the jurisdiction of the bank commissioner, the director of securities regulation, the insurance commissioner, the public utilities commission, the financial institutions and insurance regulators of other States, or federal banking or securities regulators who possess the authority to regulate unfair or deceptive trade practices must also notify the regulator which has primary regulatory authority over such trade or commerce. All other persons must notify the State attorney general. Such notice must be provide before notifying affected individuals. N.H. Rev. Stat. § 359-C:20(I)(b).

Notice sent to a regulator or the State attorney general's office must include the anticipated date of the notice to the individuals and the approximate number of individuals in New Hampshire who will be notified. The notifying person is not required to provide the names of the individuals entitled to receive the notice or any personal information relating to them. N.H. Rev. Stat. § 359-C:20(I)(b).

If the breach affects a person or business that maintains personal information, that person or business must notify the owner or licensee of that information of the breach if the personal information was acquired by an unauthorized person. N.H. Rev. Stat. § 359-C:20(I)(c).

If a person is required to notify more than 1,000 consumers of a breach of security pursuant to the statute, the person shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis 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 person is not required to provide to any consumer reporting agency the names of the consumers entitled to receive the notice or any personal

information relating to them. This requirement does not apply to a person who is subject to Title V of the Gramm, Leach-Bliley Act. N.H. Rev. Stat. § 359-C:20(VI).

WHEN MUST NOTICE BE SENT?

Notification to affected individuals, primary regulators, or the State attorney general must be provided as quickly as possible. N.H. Rev. Stat. § 359-C:20(I).

Notification to the owner or licensee of personal information by a person or business that maintains the information must be provided immediately following discovery of the breach. N.H. Rev. Stat. § 359-C:20(I).

Notification may be delayed if a law enforcement agency, or national or homeland security agency determines that the notification will impede a criminal investigation or jeopardize national or homeland security. N.H. Rev. Stat. § 359-C:20(II).

IN WHAT FORM AND MANNER MUST NOTICE BE SENT?

The notice required under this section must be provided by one of the following methods:

(1) written notice;

(2) electronic notice, if the agency or business' primary means of communication with affected individuals is by electronic means;

(3) telephonic notice, provided that a log of each such notification is kept by the notifying person or business;

(4) substitute notice, if the person demonstrates: (A) that the cost of providing notice would exceed $5,000, (B) that the affected class of subject individuals to be notified exceeds 1,000, or (C) that the person does not have sufficient contact information or consent to provide notice pursuant to methods (i)-(iii); or

(5) notice pursuant to the person's internal notification procedures maintained as part of an information security policy for the treatment of personal information.

Substitute notice must consist of all of the following:

(1) e-mail notice when the person has an e-mail address for the affected individuals;

(2) conspicuous posting of the notice on the person's business website, if the person maintains one; and

(3) notification to major Statewide media.

N.H. Rev. Stat. § 359-C:20(III).

WHAT MUST THE NOTICE SAY?

Notice under this section must include at a minimum:

(1) a description of the incident in general terms;

(2) the approximate date of breach;

(3) the type of personal information obtained as a result of the security breach; and

(4) the telephonic contact information of the notifying person.

N.H. Rev. Stat. § 359-C:20(IV).

ARE THERE ANY EXEMPTIONS?

Any person engaged in trade or commerce that is subject to N.H. Rev. Stat. § 358-A:3(I) (trade or commerce that is subject to the jurisdiction of the bank commissioner, the director of securities regulation, the insurance commissioner, the public utilities commission, the financial institutions and insurance regulators of other States, or federal banking or securities regulators who possess the authority to regulate unfair or deceptive trade practices) and which maintains procedures for security breach notification pursuant to the laws, rules, regulations, guidance, or guidelines issued by a State or federal regulator shall be deemed to be in compliance if such person acts in accordance with such laws, rules, regulations, guidance, or guidelines. N.H. Rev. Stat. § 359-C:20(V).

WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

The State attorney general shall enforce the provisions of this statute pursuant to § 358-A:4. N.H. Rev. Stat. § 359-C:21(II).

The State attorney general may bring an action for a temporary or permanent injunction and for an order of restitution of money or property to any injured person or class of persons. N.H. Rev. Stat. § 358-A:4(III)(a).

The State attorney general may also seek civil penalties up to $10,000 for each violation, provided the process of appeal has been exhausted. N.H. Rev. Stat. § 358-A:4(III)(b).

Any person injured by any violation under the statute may bring a civil action for damages and equitable relief, including an injunction. If the court finds for the plaintiff, recovery shall be in the amount of actual damages. If the court finds the violation was willful or knowing, it shall award as much as three times, but not less than two times, such amount. A prevailing plaintiff shall also be awarded the costs of the suit and reasonable attorney's fees. Injunctive relief shall be available to private individuals without bond, subject to the discretion of the court. N.H. Rev. Stat. § 359-C:21(I).

ARE THERE ANY DATA SECURITY REQUIREMENTS IMPOSED?

No.

ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

Yes.

Student and Teacher Information:

N.H. Rev. Stat. §§ 189:65-189:66 imposes requirements on the New Hampshire Department of Education pertaining to the personal information of students or teachers.

"Student personally-identifiable data" is defined as:

(1) the student's name;

(2) the name of the student's parents or other family members;

(3) the address of the student or student's family;

(4) indirect identifiers, including the student's date of birth, place of birth, Social Security number, e-mail, social media address, or other electronic address, telephone number, credit card account number, insurance account number, and financial services account number; or

(5) other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty.

"Teacher personally-identifiable data" or "teacher data," which shall apply to teachers, paraprofessionals, principals, school employees, contractors, and other administrators, is defined as:

(1) Social Security number;

(2) date of birth;

(3) personal street address, e-mail address, or telephone numbers;

(4) performance evaluations; or

(5) other information that, alone or in combination, is linked or linkable to a specific teacher, paraprofessional, principal, or administrator that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify any with reasonable certainty.

The New Hampshire Department of Education is required to create a detailed data security plan that must require notification as soon as practicable to:

(1) any teacher or student whose personally identifiable information could reasonably be assumed to have been part of any data security breach, 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;

(2) the Governor, State Board, Senate President, Speaker of the House of Representatives, Chairperson of the Senate Committee with primary jurisdiction over education, Chairperson of the House Committee with primary jurisdiction over education, Legislative Oversight Committee established, and Commissioner of the Department of Information Technology; and

Require the New Hampshire Department of Education to issue an annual data security breach report to the Governor, State Board, Senate President, Speaker of the House of Representatives, chairperson of the Senate Committee with primary jurisdiction over education, chairperson of the House Committee with primary jurisdiction over education, Legislative Oversight Committee established in RSA 193-C:7, and Commissioner of the Department of Information Technology. The breach report must be posted to the Department's public website and must not include any information that itself would pose a security threat to a database or data system. The report must include:

(1) the name of the organization reporting the breach;

(2) any types of personal information that were or are reasonably believed to have been the subject of a breach;

(3) the date, estimated date, or date range of the breach;

(4) a general description of the breach incident;

(5) the estimated number of students and teachers affected by the breach, if any; and

(6) information about what the reporting organization has done to protect individuals whose information has been breached.

N.H. Rev. Stat. § 189:66(III).

The New Hampshire Department of Education must establish minimum standards for maintaining the privacy and security of student and employee data, based on best practices, for local education agencies. Each local education agency must develop a data and privacy governance plan, to be updated annually, which must be presented to the School Board for review and approval by June 30, 2019. The plan must include:

(1) an inventory of all software applications, digital tools, and extensions, including users of the applications, the provider, purpose, publisher, privacy Statement, and terms of use;

(2) a review of all software applications, digital tools, and extensions and an assurance that they meet or exceed standards set by the State's Department of Education;

(3) policies and procedures for access to data and protection of privacy for students and staff including acceptable use policy for applications, digital tools, and extensions;

(4) a response plan for any breach of information; and

(5) a requirement for a service provider to meet or exceed standards for data protection and privacy.

2018 New Hampshire Laws Ch. 252 (H.B. 1612).

Insurance:

N.H. Code Admin. R. Ins. § 3702.01, *et seq.*, sets forth specific requirements for licensees with respect to the nonpublic personal information of a customer of a licensee.

"Licensees" is defined as licensed insurers, producers and other persons licensed, authorized, or registered, or so required to be. The definition excludes a purchasing group or an unauthorized insurer in regard to the excess line business conducted pursuant to N.H. Rev. Stat. § 406-B. N.H. Code Admin. R. Ins. §§ 3001.04(q); 3702.02(d).

When a licensee becomes aware of an incident of unauthorized access to customer information, the licensee shall immediately investigate to promptly determine the likelihood that the information has been or will be misused. N.H. Code Admin. R. Ins 3702.03(a).

If a licensee determines that misuse of its customer information has occurred or is reasonably likely to occur or if a determination cannot be made, it must notify: (1) the New Hampshire Insurance Department as soon as possible; and (2) affected customers in writing as soon as possible, but no later than 30 days. However, the customer notice shall not be issued until the earlier of:

(6) five days after the licensee submits the notice to the New Hampshire Insurance Department for review; or

(7) receipt from the Department of approval of the written notice that has been filed.

N.H. Code Admin. R. Ins. § 3702.03.

If a licensee, based upon its investigation, can determine from its logs or other data precisely which customers' information has been improperly accessed, it may limit notification to those customers with regard to whom the licensee determines that misuse of information has occurred or is reasonably possible. If the licensee is unable to identify which specific customers' information has been accessed, it shall notify all customers by substitute notice in accordance with § 359-C:20(III)(d). N.H. Code Admin. R. Ins. § 3702.04.

Customer notice shall be given in a clear and conspicuous manner. The notice shall describe the incident in general terms, the type of customer information that was the subject of the unauthorized access or use, and the approximate date of the breach. The notice shall include a telephone number that customers may call for further information and assistance. N.H. Code Admin. R. Ins. § 3702.05.

Customer notice may be delivered by: (1) telephone, provided that the licensee maintains a log of each such notification; (2) U.S. mail; or (3) e-mail, if the customer has agreed to receive communications electronically. N.H. Code Admin. R. Ins. § 3702.06.

Medical Information:

N.H. Rev. Stat. § 332-I:1, *et seq.*, sets forth specific requirements for the maintenance of protected health information that is used or disclosed by a health care provider or a business associate of a health care provider.

"Health care provider" means any person, corporation, facility, or institution either licensed by New Hampshire or otherwise lawfully providing health care services, including, but not limited to, a physician, advanced practice registered nurse, physician assistant, hospital, office, clinic, health center or other health care facility, dentist, nurse, optometrist, pharmacist, podiatrist, physical therapist, mental health professional, care coordinator, managed care provider, or the department of health and human services, and any officer, employee, or agent of such provider acting in the course and scope of employment or agency related to or supportive of health care services. N.H. Rev. Stat. § 332-I:1(II)(b).

"Protected health information" is defined as individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. Protected health does not include education records covered by the Family Educational Rights and Privacy Act, employment records held by a covered entity in its role as employer, records on a study eighteen years or older or attending a postsecondary education that are made or maintained by a health care professional in connection with providing treatment, and anything regarding a person who has been deceased for more than 50 years. 45 C.F.R. § 160.103.

In the event of a use or disclosure of protected health information by a health care provider or their business associate for marketing or fundraising purposes in a manner not permitted under N.H. Rev. Stat. § 332-I:4 (even if permissible under federal law), the health care provider must promptly notify in writing the individuals whose protected health information was disclosed. N.H. Rev. Stat. § 332-I:5. The business associate must bear the costs of such notification if the use or disclosure was by the business associate.

An affected individual may bring a civil action for special or general damages of at least $1,000 per violation as well as costs and reasonable legal fees. N.H. Rev. Stat. Ann. § 332-I:6.

NEW JERSEY

STATUTE: N.J. Stat. §§ **56:8-161 - 56:8-163**,[72] 56:11-53 – 56:11:55.[73]

WHO MUST COMPLY?

Any business that conducts business in New Jersey, or any business or public entity that compiles or maintains computerized records that include personal information of residents of the State, including on behalf of another business or public entity. N.J. Stat. § 56:8-163(a)-(b).

"Business" is defined as a sole proprietorship, partnership, corporation, association, or other entity, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the law of any State, the United States, or of any other country, or the parent or the subsidiary of a financial institution. N.J. Stat. § 56:8-161.

"Public entity" includes the State, and any county, municipality, district, public authority, public agency, and any other political subdivision or public body in the State. N.J. Stat. § 56:8-161.

WHAT DATA IS COVERED?

An individual's first name or first initial and last name linked with any 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 or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account;

(4) user name, e-mail address, or any other account holder identifying information, in combination with any password or security question and answer that would permit access to an online account;[74] or

(5) Dissociated data that, if linked, would constitute personal information qualifies as personal information if the means to link the dissociated data is accessed in connection with access to the dissociated data.

[72] Publicly available at: *New Jersey Statutes (Unannotated)*, https://lis.njleg.state.nj.us/nxt/gateway.dll?f=templates&fn=default.htm&vid=Publish:10.1048/Enu**,** https://lis.njleg.state.nj.us/nxt/gateway.dll/statutes%2F1%2F50801%2F51179 (last visited July 9, 2019).
[73] Publicly available at: *New Jersey Revised Statutes (Unannotated)*, https://lis.njleg.State.nj.us/nxt/gateway.dll?f=templates&fn=default.htm&vid=Publish:10.1048/Enu (last visited July 9, 2019).
[74] (4) will take effect September 1, 2019.

Personal information does not include publicly available information that is lawfully made available to the general public from federal, State or local government records, or widely distributed media. N.J. Stat. § 56:8-161.

WHAT CONSTITUTES A DATA BREACH?

The unauthorized access to electronic files, media or data containing personal information that compromises the security, confidentiality or integrity of personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable. Good faith acquisition of personal information by an employee or agent of the business for a legitimate business purpose is not a breach of security, provided that the personal information is not used for a purpose unrelated to the business or subject to further unauthorized disclosure. N.J. Stat. § 56:8-161.

WHO MUST BE NOTIFIED?

The Division of State Police in the Department of Law and Public Safety must be notified for purposes of investigation and handling before the business or public entity discloses the breach to any affected customer. N.J. Stat. § 56:8-163(c).

Any customer (any individual who provides personal information to a business) who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person. Disclosure of a breach to a customer is not required if the business or public entity establishes that misuse of the information is not reasonably possible. Any determination shall be documented in writing and retained for 5 years. N.J. Stat. § 56:8-163(a).

Any business or public entity that compiles or maintains personal information on behalf of another business or public entity must notify that business or public entity, who must notify its affected New Jersey customers, of the breach, if the personal information was, or is reasonably believed to have been, accessed by an unauthorized person. N.J. Stat. § 56:8-163(b).

In the event that a business or public entity discovers circumstances requiring notification of more than 1,000 persons at one time, the business or public entity must also notify, without unreasonable delay, all consumer reporting agencies that compile or maintain files on consumers on a nationwide basis of the timing, distribution and content of the notices. N.J. Stat. § 56:8-163(f).

WHEN MUST NOTICE BE SENT?

The disclosure to an affected customer must be made in the most expedient time possible and without unreasonable delay following discovery or notification of the breach, consistent with the legitimate needs of law enforcement, or any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system. N.J. Stat. § 56:8-163(a).

The disclosure to an affected business or public entity by a business or public entity that compiles or maintains public information on its behalf must be made immediately following discovery of a breach. N.J. Stat. § 56:8-163(a).

Notification may be delayed if a law enforcement agency determines that the notification will impede a criminal or civil investigation and that agency has made a request that the notification be delayed. N.J. Stat. § 56:8-163(c).

IN WHAT FORM AND MANNER MUST NOTICE BE SENT?

Notice must be provided by one of the following methods:

(1) written notice;

(2) electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in § 101 of the federal Electronic Signatures in Global and National Commerce Act; or

(3) substitute notice, if the business or public entity demonstrates: (1) that the cost of providing notice would exceed $250,000; (2) that the affected class of subject persons to be notified exceeds 500,000; or (3) the business or public entity does not have sufficient contact information.

Substitute notice shall consist of all of the following:

(1) e-mail notice when the business or public entity has an e-mail address;

(2) conspicuous posting of the notice on the website of the business or public entity, if the business or public entity maintains one; and

(3) notification to major Statewide media.

N.J. Stat. § 56:8-163(d).

Notwithstanding the methods in which notice must be provided above, in the case of a breach of security involving a user name or password, in combination with any password or security question and answer that would permit access to an online account, and no other personal information as defined in section 10 of P.L.2005, c.226 (C.56:8-161), the business or public entity may provide the notification in electronic or other form that directs the customer whose personal information has been breached to promptly change any password and security question or answer, as applicable, or to take other appropriate steps to protect the online account with the business or public entity and all other online accounts for which the customer uses the same user name or email address and password or security question or answer.

Any business or public entity that furnishes an e-mail account shall not provide notification to the e-mail account that is subject to a security breach. The business or public entity shall provide notice by another method described in this section or by clear and conspicuous notice delivered to the customer online when the customer is connected to the online account from an Internet Protocol address or online location from which the business or public entity knows the customer customarily accesses the account.

N.J. Stat. § 56:8-163(g).

WHAT MUST THE NOTICE SAY?

The statute does not address the contents of the notification.

ARE THERE ANY EXEMPTIONS?

A business or public entity that maintains its own notification procedures as part of an information security policy for the treatment of personal information, and is otherwise consistent with the requirements of the statute, shall be deemed to comply with the notification requirements of the statute if the business or public entity notifies subject customers in accordance with its policies in the event of a breach of security of the system. N.J. Stat. § 56:8-163(e).

WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

Any person aggrieved by a violation of the statute may bring an action for damages or to enjoin further violations. In the event the plaintiff establishes a violation of the statute, the court may award actual damages sustained, or $500 for each violation, whichever amount is greater, together with costs of suit and reasonable attorney's fees. N.J. Stat. § 56:8-159(a)-(b).

A violation of the statute constitutes an unlawful practice under N.J. Stat. § 56-8-1, *et seq.*, and will be subject to all remedies available under that chapter. N.J. Stat. § 56:8-160.

ARE THERE ANY DATA SECURITY REQUIREMENTS IMPOSED?

A business or public entity must destroy, or arrange for the destruction of, a customer's records within its custody or control containing personal information, which is no longer to be retained by the business or public entity, by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable, undecipherable or non-reconstructable through generally available means. N.J. Stat. § 56:8-162.

ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

The Personal Information Privacy and Protection Act places restrictions on a retailers' ability to collect and use personal information gleaned from driver's licenses and other identification cards. N.J. Stat. Ann. §§ 56:11-53 – 56:11-55.

Retailers may scan customers' identification cards for certain enumerated purposes related to verification, fraud prevention, business interests, and statutory obligations to record, retain, or transmit information. The information collected must be limited to the person's name, address, date of birth, the issuing State, and identification card number. N.J. Stat. Ann. § 56:11-54(b)-(c).

Retailers must securely store any information retained and report any security breaches to the Division of State Police in the Department of Law and Public Safety and any affected resident in accordance with the data breach notification statute. N.J. Stat. Ann. § 56:11-54.

Any person who violates these provisions will be subject to a civil penalty of $2,500 for the first violation, and $5,000 for any subsequent violation. Any person affected by a violation may bring a private action to recover damages. N.J. Stat. Ann. § 56:11-55.

NEW MEXICO

STATUTE: N.M. Stat. Ann. §§ 57-12C-1, *et seq.*[75]

WHO MUST COMPLY?

A person that owns or licenses elements that include personal identifying information of a New Mexico resident or any person that is licensed to maintain or possess computerized data containing personal identifying information of a New Mexico resident. N.M. Stat. Ann. § 57-12C-6.

WHAT DATA IS COVERED?

Personal identifying information, which is an individual's first name or first initial and last name in combination with one or more of the following data elements that relate to the individual, when the data elements are not protected through encryption or redaction or otherwise rendered unreadable or unusable:

(1) Social Security number;

(2) driver's license number;

(3) government-issued identification number;

(4) account number, credit card number or debit card number in combination with any required security code, access code or password that would permit access to a person's financial account; or

(5) biometric data.

N.M. Stat. Ann. § 57-12C.

Personal identifying information does not include data that is lawfully obtained from publicly available sources or from federal, State or local government records lawfully made available to the general public. N.M. Stat. Ann. § 57-12C(2).

WHAT CONSTITUTES A DATA BREACH?

The unauthorized acquisition of unencrypted computerized data, or of encrypted computerized data and the confidential process or key used to decrypt the encrypted computerized data, that compromises the security, confidentiality or integrity of personal identifying information maintained by a person. A breach does not include the good-faith acquisition of personal identifying information by an employee or agent of a person for a legitimate business purpose of

[75] Publicly available at: *Data Breach Notification, https://laws.nmonesource.com/w/nmos/Chapter-57-NMSA-1978#!fragment/zoupio-Toc12632020/BQCwhgziBcwMYgK4DsDWszIQewE4BUBTADwBdoAvbRABwEtsBaAfX2zgEYAmANgGYuABiEBKADTJspQhACKiQrgCe0AOSqxEOLmwAbXQGEkaaAEJkmwmFwJ5ilesvWEAZTykAQioBKAUQAyvgBqAIIAcga+YqRgAEbQpOwiIkA* (last visited July 8, 2019).

the person, provided that the personal identifying information is not subject to further unauthorized disclosure. N.M. Stat. Ann. § 57-12C-2(D).

WHO MUST BE NOTIFIED?

A resident whose personal identifying information is reasonably believed to have been subject to a security breach. N.M. Stat. Ann. § 57-12C-6(A).

Any person that is licensed to maintain or possess computerized data containing personal identifying information of a New Mexico resident must notify the owner or licensee of the information of any security breach. N.M. Stat. Ann. § 57-12C-6(C).

When notification to more than 1,000 residents is required as a result of a single security breach, the office of the attorney general and major consumer reporting agencies that compile and maintain files on consumers on a nationwide basis must be notified. Notice to the attorney general and consumer reporting agencies must include the number of New Mexico residents that received notification and provide a copy of the notification sent to affected residents. N.M. Stat. Ann. § 57-12C-10.

WHEN MUST NOTICE BE SENT?

Notification must be made in the most expedient time possible, but not later than 45 calendar days following discovery of the security breach. N.M. Stat. Ann. § 57-12C-6(A).

Notification may be delayed: (1) if a law enforcement agency determines that the notification will impede a criminal investigation; or (2) as necessary to determine the scope of the security breach and restore the integrity, security and confidentiality of the data system. N.M. Stat. Ann. § 57-12C-9.

IN WHAT FORM AND MANNER MUST NOTICE BE SENT?

Notice to affected residents must be provided by:

(1) United States mail;

(2) electronic notification, if the person required to make the notification primarily communicates with the New Mexico resident by electronic means or if the notice provided is consistent with the requirements of 15 U.S.C. Section 7001; or

(3) a substitute notification, if the person demonstrates that:

  (a) the cost of providing notification would exceed $100,000;

  (b) the number of residents to be notified exceeds 50,000; or

  (c) the person does not have on record a physical address or sufficient contact information for the residents required to be notified.

Substitute notification shall consist of:

(1) sending electronic notification to the e-mail address of those residents for whom the person has a valid e-mail address;

(2) posting notification of the security breach in a conspicuous location on the website of the person required to provide notification if one is maintained; and

(3) sending written notification to the office of the attorney general and major media outlets in New Mexico. N.M. Stat. Ann. § 57-12C-6(D)-(E).

WHAT MUST THE NOTICE SAY?

Notification shall contain:

(1) the name and contact information of the notifying person;

(2) a list of the types of personal identifying information that are reasonably believed to have been the subject of a security breach, if known;

(3) the date, estimated date, or the range of dates within which the security breach occurred, if known;

(4) a general description of the security breach incident;

(5) the toll-free telephone numbers and addresses of the major consumer reporting agencies;

(6) advice that directs the recipient to review personal account Statements and credit reports, as applicable, to detect errors resulting from the security breach; and

(7) advice that informs the recipient of the notification of the recipient's rights pursuant to the federal Fair Credit Reporting Act.

N.M. Stat. Ann. § 57-12C-7.

ARE THERE ANY EXEMPTIONS?

Notification is not required if, after an appropriate investigation, a person determines that the security breach does not give rise to a significant risk of identity theft or fraud. N.M. Stat. Ann. § 57-12C-6(B)-(C).

The statute does not apply to a person subject to the federal Gramm–Leach–Bliley Act or the federal Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). N.M. Stat. Ann. § 57-12C-8.

The statute does not apply to the State or any of its political subdivisions. N.M. Stat. Ann. § 57-12C-12.

WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

The State attorney general may bring an action on the behalf of individuals and the State for a violation of the statute. In any such action, the court may issue an injunction and award damages for actual costs or losses, including consequential financial losses. N.M. Stat. Ann. § 57-12C-11(A)-(B).

If the court determines that a person violated the statute knowingly or recklessly, the court may impose a civil penalty of the greater of: (1) $25,000; or (2) in the case of failed notification, $10 per instance of failed notification, provided such fines will not exceed $150,000. N.M. Stat. Ann. § 57-12C-11(C).

The statute does not address a private right of action.

ARE THERE ANY DATA SECURITY REQUIREMENTS IMPOSED?

A person that owns or licenses records containing personal identifying information of a New Mexico resident must arrange for proper disposal of the records when they are no longer reasonably needed for business purposes. "Proper disposal" means shredding, erasing or otherwise modifying the personal identifying information contained in the records to make the personal identifying information unreadable or undecipherable. N.M. Stat. Ann. § 57-12C-3.

A person that owns or licenses personal identifying information of a New Mexico resident must implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal identifying information from unauthorized access, destruction, use, modification or disclosure. N.M. Stat. Ann. § 57-12C-4.

A person that discloses personal identifying information of a New Mexico resident pursuant to a contract with a service provider must contractually require that the service provider implement and maintain reasonable security procedures and practices appropriate to the nature of the personal identifying information and to protect it from unauthorized access, destruction, use, modification or disclosure. N.M. Stat. Ann. § 57-12C-5.

ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

No.

NEW YORK

STATUTE: N.Y. Gen. Bus. Law §§ 399-h,[76] 899-aa;[77] N.Y. State Tech. Law § 208;[78] N.Y. Comp. Codes R. & Regs. tit. 23, § 500;[79] N.Y.C. Admin. Code § 20-117.[80]

WHO MUST COMPLY?

Any person or business that conducts business in New York State, and which owns, licenses, or maintains computerized data which includes private information. Any person or business that maintains computerized data which includes private information that such person or business does not own. N.Y. Gen. Bus. Law §§ 899-aa(2)-(3).

State entities are subject to substantially similar notification requirements. N.Y. State Tech. Law § 208. "State entity" is defined as any State board, bureau, division, committee, commission, council, department, public authority, public benefit corporation, office or other governmental entity performing a governmental or proprietary function for New York, but does not include the judiciary or any cities, counties, municipalities, villages, towns, and other local agencies. N.Y. State Tech. Law § 208(1)(c).

WHAT DATA IS COVERED?

Any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted, or encrypted with an encryption key that has also been acquired:

(1) Social Security number;

(2) driver's license number or non-driver identification card number; or

(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.

(4) Private information does not include publicly available information which is lawfully made available to the general public from federal, State, or local government records. N.Y. Gen. Bus. Law §§ 899-aa(1)(a), (b).

---

[76] Publicly available at *Laws of New York*, http://public.leginfo.State.ny.us/lawssrch.cgi?NVLWO: (last visited August 26, 2018).
[77] Publicly available at *Laws of New York*, http://public.leginfo.State.ny.us/lawssrch.cgi?NVLWO: (last visited August 26, 2018).
[78] Publicly available at *Laws of New York*, http://public.leginfo.State.ny.us/lawssrch.cgi?NVLWO: (last visited August 26, 2018).
[79] Publicly available at *Dept. of Financial Services*, https://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf (last visited August 26, 2018).
[80] Publicly available at *New York City Administrative Code*, http://library.amlegal.com/nxt/gateway.dll/New%20York/admin/newyorkcityadministrativecode?f=templates$fn=default.htm$3.0$vid=amlegal:newyork_ny (last visited August 26, 2018).

The statute does not apply if the data subject to the breach was encrypted. N.Y. Gen. Bus. Law § 899-aa(1)(b). But this exception does not apply if the encryption is compromised.

WHAT CONSTITUTES A DATA BREACH?

The unauthorized acquisition, or acquisition without valid authorization, of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a business. Good faith acquisition of personal information by an employee or agent of the business for the purposes of the business is not a breach of the security of the system, provided that the private information is not used or subject to unauthorized disclosure. N.Y. Gen. Bus. Law § 899-aa(1)(c).

WHO MUST BE NOTIFIED?

Any person or business which conducts business in New York, and which owns or licenses computerized data which includes private information must disclose upon discovery or notification any breach to any resident of New York State whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization. N.Y. Gen. Bus. Law § 899-aa(2).

Any person or business which maintains computerized data which includes private information they do not own 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. N.Y. Gen. Bus. Law § 899-aa(3).

Any person or business required to notify affected residents must also notify the State attorney general, the department of State, and the division of policy as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice must be made without delaying notice to affected residents. N.Y. Gen. Bus. Law §§ 899-aa(8)(a).

State entities are required to notify the State office of information technology services (instead of the division of policy) and must consult with the office to determine the scope of the breach and restoration measures. N.Y. Gen. Bus. Law §§ 208(2), (7)(a).

In the event more than 5,000 residents are required to be notified at one time, the person or business must also notify consumer reporting agencies as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice must be made without delaying notice to affected residents. N.Y. Gen. Bus. Law §§ 899-aa(8)(b).

WHEN MUST NOTICE BE SENT?

Notice to affected residents must be provided 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. N.Y. Gen. Bus. Law §§ 899-aa(2), (4).

Notice to an affected owner or licensee by a person or business who maintains their personal information must be provided immediately following discovery but may be delayed if a law

enforcement agency determines such notice would impede a criminal investigation. N.Y. Gen. Bus. Law §§ 899-aa(3), (4).

IN WHAT FORM AND MANNER MUST NOTICE BE SENT?

Notice shall be provided by one of the following methods:

(1) written notice;

(2) electronic notice, provided that the person to whom notice is required has expressly consented to receiving notice in electronic form and a log of each such notification is kept by the person or business who notifies affected persons in such form;

(3) telephone notification, provided that a log of each such notification is kept by the person or business who notifies affected persons; or

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

Substitute notice shall consist of all of the following:

(1) e-mail notice when such business has an e-mail address for the subject persons;

(2) conspicuous posting of the notice on such business's website, if such business maintains one; and

(3) notification to major Statewide media.

N.Y. Gen. Bus. Law § 899-aa(5).

WHAT MUST THE NOTICE SAY?

Any notice must include: (1) contact information for the person or business making the notification; and (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, acquired. N.Y. Gen. Bus. Law § 899-aa(7).

ARE THERE ANY EXEMPTIONS?

The statute does not address any exemptions.

WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

The State attorney general may enforce the statute and seek an injunction and damages for actual costs or losses incurred by a person entitled to notice but who did not receive it, including

consequential financial losses. If the court determines that a person or business violated the statute knowingly or recklessly, the court may impose a civil penalty of the greater of $5,000 or up to $10 per instance of failed notification, provided that the latter amount shall not exceed $150,000. N.Y. Gen. Bus. Law § 899-aa(6)(a).

Any action under the act must be brought within 2 years immediately after the date of the act complained of or the date of discovery. N.Y. Gen. Bus. Law § 899-aa(6)(c).

There is no private right of action.

ARE THERE ANY DATA SECURITY REQUIREMENTS IMPOSED?

No person, business, firm, partnership, association, or corporation, not including the State or its political subdivisions, may dispose of a record containing personal identifying information unless it, or another person with whom it has contracted, does any of the following:

(1) shreds the record before the disposal of the record;

(2) destroys the personal identifying information contained in the record;

(3) modifies the record to make the personal identifying information unreadable; or

takes actions consistent with commonly accepted industry practices that it reasonably believes will ensure that no unauthorized person will have access to the personal identifying information contained in the record.

N.Y. Gen. Bus. Law § 399-h(2).

These disposal requirements do not apply to any individual person unless they are conducting business for profit. N.Y. Gen. Bus. Law § 399-h(2).

For purposes of N.Y. Gen. Bus. Law § 399-h, "personal identifying information" means any personal information (any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person) in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted, or encrypted with an encryption key that is included in the same record as the encrypted personal information or data element:

(1) Social Security number;

(2) driver's license number or non-driver identification card number; or

(3) mother's maiden name, financial services account number or code, savings account number or code, checking account number or code, debit card number or code, automated teller machine number or code, electronic serial number, or any number or code which may be used alone or in conjunction with any other information to assume the identity of another person or access financial resources or credit of another person.

N.Y. Gen. Bus. Law § 399-h(1)(c)-(e).

The State attorney general may seek an injunction and a civil penalty of not more than $5,000 for a violation of these disposal requirements. It will be an affirmative defense if a business can show that it used due diligence in its attempt to properly dispose of such records. N.Y. Gen. Bus. Law § 399-h(3).

ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

Licensees:

New York City Administrative Code § 20-117 sets forth notification requirements in the event of a breach of security for persons required to be licensed by New York City's Department of Consumer Affairs or pursuant to State laws enforced by the Department.

"Personal identifying information" is broadly defined to include any person's date of birth, Social Security number, driver's license number, non-driver photo identification card number, financial services account number or code, savings account number or code, checking account number or code, brokerage account number or code, credit card account number or code, debit card number or code, automated teller machine number or code, personal identification number, mother's maiden name, computer system password, electronic signature or unique biometric data that is a fingerprint, voice print, retinal image or iris image of another person. The term applies to any such data regardless of the method by which it is maintained. New York City Admin. Code § 20-117(a)(1).

Any covered licensee that owns, leases, or maintains but does not own data that includes personal identifying information must immediately disclose any breach of security to the Department of Consumer Affairs and police department following discovery by, or notification to, a supervisor or manager if personal identifying information is reasonably believed to have been acquired by an unauthorized person. New York City Admin. Code § 20-117(b).

Subsequent to notification to the Department and police department, any covered licensee that owns or leases data that includes personal identifying information must disclose, following discovery by, or notification to, a supervisor or manager, any breach of security to any person whose personal identifying information was, or is reasonably believed to have been, acquired by an unauthorized person. New York City Admin. Code § 20-117(c).

Subsequent to notification to the Department and police department, any covered licensee that maintains but does not own data that includes personal identifying information must disclose, following discovery by, or notification to, a supervisor or manager, any breach of security to the owner, lessor, or licensor of the data if the personal identifying information was, or is reasonably believed to have been, acquired by an unauthorized person. New York City Admin. Code § 20-117(d).

Notification to affected individuals, owners, lessors, and licensors must be provided as soon as practicable by one of the following means:

(1) written notice to the individual at their last known address;

(2) verbal notification to the individual by telephonic communication;

(3) electronic notification to the individual at their last known e-mail address; or

(4) if disclosure pursuant to (1)-(3) be impracticable or inappropriate given the circumstance of the breach and the identity of the victim, disclosure may be made by a mechanism of the licensee's choosing, provided such mechanism is reasonably targeted to the individual in a manner that does not further compromise the integrity of the personal information disclosed and has been approved, or is in compliance with rules promulgated, by the Commissioner of Consumer Affairs.

New York City Admin. Code § 20-117(e)-(f).

Any covered licensee that discards any records of an individual's personal identifying information must do so in a manner intended to prevent retrieval of the information contained therein or thereon. New York City Admin. Code § 20-117(g).

Any covered licensee who violates any provisions of section 20-117 will be liable for a fine up to $500 and a civil penalty up to $100 per violation. New York City Admin. Code § 20-117(h).

Entities Subject to the Banking Law, Insurance Law, or Financial Services Law:

23 NYCRR Part 500.00 imposes cybersecurity requirements for any individual or any non-governmental entity operating under, or required to operate under, a license or similar permit under the Banking Law, the Insurance Law or the Financial Services Law.

Requirements for covered entities include but are not limited to:

(1) maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the covered entity's information systems (23 NYCRR § 500.02);

(2) implement and maintain a written cybersecurity policy or policies setting forth the covered entity's policies and procedures for the protection of its information systems and nonpublic information stored thereon (23 NYCRR § 500.03);

(3) designate a Chief Information Security Officer for overseeing and implementing the covered entity's cybersecurity program and enforcing its cybersecurity policy (23 NYCRR § 500.04);

(4) conduct monitoring and testing to assess the effectiveness of the covered entity's cybersecurity program, including annual penetrating testing and bi-annual vulnerability assessments (23 NYCRR § 500.05);

(5) conduct a periodic documented risk assessment of the covered entity's information systems in accordance with its written policies and procedures (23 NYCRR § 500.09);

(6) implement written policies and procedures designed to ensure the security of information systems and nonpublic information that are accessible to, or held by, third party service providers (23 NYCRR § 500.11);

(7) maintain policies and procedures for the secure disposal on a periodic basis of any nonpublic information that is no longer necessary for business operations or for other legitimate business purposes (23 NYCRR § 500.13);

(8) establish a written incident response plan designed to promptly respond to, and recover from, any Cybersecurity Event materially affecting the confidentiality, integrity or availability of the covered entity's information systems or the continuing functionality of any aspect of the entity's business or operations (23 NYCRR § 500.16).

Covered entities must notify the Superintendent of Financial Services as promptly as possible but in no event later than 72 hours from a determination that either of the following "Cybersecurity Events" have occurred:

(1) Cybersecurity Events impacting the covered entity of which notice is required to be provided to any government body, self-regulatory agency or any other supervisory body; or

(2) Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operation(s) of the covered entity.

23 NYCRR § 500.17(a).

For purposes of these requirements, "Cybersecurity Event" means any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt, or misuse an information system or information stored on such information system. 23 NYCRR § 500.01(d).

Covered entities must submit a written Statement each year to the Superintendent certifying that the covered entity is in compliance with these requirements. Covered entities must maintain for purposes of examination all records, schedules, and data supporting this certificate for a period of five years. 23 NYCRR § 500.17(b).

Covered Entities will be exempt from some or all of the Regulations if they meet any of the following criteria:

(a) have fewer than 10 employees, which number will include all employees and independent contractors of the Covered Entity or any affiliate(s) of the Covered Entity located in New York and responsible for the Covered Entity's business;

(b) had less than $5 million in gross annual revenue in each of the last three fiscal years from New York business operations of the Covered Entity or its affiliates; or

(c) has less than $10 million in year-end total assets, calculated in accordance with

GAAP, including assets of all affiliates.

23 NYCCR 500.19(a).

The last transitional date is March 1, 2019, by which date covered entities must be fully compliant with all requirements under 23 NYCRR Part 500.00. 23 NYCRR § 500.22.

NORTH CAROLINA

STATUTE: N.C. Gen. Stat. §§ 75-61,[81] 75-64,[82] 75-65.[83]

WHO MUST COMPLY?

Any business that owns, licenses, maintains, or possesses personal information of residents of North Carolina or any business that conducts business in North Carolina that owns, licenses, maintains, or possesses personal information in any form (whether computerized, paper, or otherwise). N.C. Gen. Stat. § 75-65(a), (b).

WHAT DATA IS COVERED?

A person's first name or first initial and last name in combination with identifying information listed below:

(1) Social Security or employer taxpayer identification numbers;

(2) driver's license, State identification card, or passport numbers;

(3) checking account numbers;

(4) savings account numbers;

(5) credit card numbers;

(6) debit card numbers;

(7) Personal Identification (PIN) Code, or a numeric and/or alphabetical code assigned to the cardholder of a financial transaction card by the issuer to permit authorized electronic use of that financial transaction card;

(8) electronic identification numbers, electronic mail names or addresses, Internet account numbers, or Internet identification names;

(9) digital signatures;

(10) any other numbers or information that can be used to access a person's financial resources;

---

[81] Publicly available at: *Definitions*, www.ncga.state.nc.us, http://www.ncga.state.nc.us/EnactedLegislation/Statutes/HTML/BySection/Chapter_75/GS_75-61.html (last visited Jul 19, 2019).

[82] Publicly available at: *Destruction of personal information records*, www.ncga.state.nc.us, https://www.ncleg.net/EnactedLegislation/Statutes/HTML/BySection/Chapter_75/GS_75-64.html (last visited July 19, 2019).

[83] Publicly available at: *Protection from security breaches*, www.ncga.state.nc.us, http://www.ncga.state.nc.us/EnactedLegislation/Statutes/HTML/BySection/Chapter_75/GS_75-65.html (last visited July 19, 2019).

(11) biometric data;

(12) fingerprints;

(13) passwords; or

(14) parent's legal surname prior to marriage.

N.C. Gen. Stat. §§ 14-113.20(b), 75-61(10).

Personal information does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, including name, address, and telephone number, and does not include information made lawfully available to the general public from federal, state, or local government records. N.C. Gen. Stat. § 75-61(10).

For purposes of determining when notification must be provided, personal information does not include electronic identification numbers, electronic mail names or addresses, Internet account numbers, Internet identification names, parent's legal surname prior to marriage, or a password unless this information would permit access to a person's financial account or resources. N.C. Gen. Stat. Ann. § 75-65(a).

WHAT CONSTITUTES A DATA BREACH?

Any incident of unauthorized access to and acquisition of unencrypted and unredacted records or data containing personal information where illegal use of the personal information has occurred or is reasonably likely to occur or that creates a material risk of harm to a consumer. Any incident of unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential process or key shall constitute a security breach. N.C. Gen. Stat. § 75-61(14).

Good faith acquisition of personal information by an employee or agent of the business for a legitimate purpose is not a security breach, provided that the personal information is not used for a purpose other than a lawful purpose of the business and is not subject to further unauthorized disclosure. N.C. Gen. Stat. § 75-61(14).

The statute defines "encryption" as the use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without use of a confidential process or key. N.C. Gen. Stat. § 75-61(8).

WHO MUST BE NOTIFIED?

Affected persons must be notified. N.C. Gen. Stat. Ann. § 75-65(a).

If a business is required to provide notice to affected persons, the business must notify, without unreasonable delay, the Consumer Protection Division of the state attorney general's office of the nature of the breach, the number of consumers affected by the breach, steps taken to investigate the breach, steps taken to prevent a similar breach in the future, and information regarding the timing, distribution, and content of the notice. N.C. Gen. Stat. Ann. § 75-65(e1).

If a business is required to provide notice to more than 1,000 persons at one time, the business must notify, without unreasonable delay, the Consumer Protection Division of the state attorney general's office and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution, and content of the notice. N.C. Gen. Stat. § 75-65(f).

Any business that maintains or possesses records or data containing personal information of residents of North Carolina that the business does not own or license or any business that conducts business in North Carolina that maintains or possesses records or data containing personal information that the business does not own or license must notify the owner or licensee of the information. N.C. Gen. Stat. Ann. § 75-65(b).

WHEN MUST NOTICE BE SENT?

Notice to affected persons must be made without unreasonable delay, consistent with the legitimate needs of law enforcement, and consistent with any measures necessary to determine sufficient contact information, determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system. N.C. Gen. Stat. § 75-65(a).

Notice to an affected owner or licensee by a business that maintains or possesses their personal information must be made immediately following discovery of the breach, consistent with the legitimate needs of law enforcement. N.C. Gen. Stat. § 75-65(b).

Notice may be delayed if a law enforcement agency informs the business that notification may impede a criminal investigation or jeopardize national or homeland security. Notice must be provided without unreasonable delay after the law enforcement agency communicates to the business its determination that notice will no longer impede the investigation or jeopardize national or homeland security. N.C. Gen. Stat. Ann. § 75-65(c).

IN WHAT FORM AND MANNER MUST NOTICE BE SENT?

Notice to affected persons must be provided by one of the following methods:

(3) written notice;

(4) electronic notice, for those persons for whom the business has a valid e-mail address and who have agreed to receive communications electronically if the notice provided is consistent with the provisions regarding electronic records and signatures for notices legally required to be in writing set forth in 15 U.S.C. § 7001; or

(5) telephonic notice, provided that contact is made directly with the affected persons; or

(6) substitute notice, (A) if the business demonstrates that the cost of providing notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000, (B) if the business does not have sufficient contact information or consent to provide notice pursuant to (1)-(3), for only those affected persons

without sufficient contact information or consent, or (C) if the business is unable to identify particular affected persons, for only those unidentifiable affected persons.

N.C. Gen. Stat. § 75-65(e).

Substitute notice must consist of all the following:

(1) e-mail notice when the business has an electronic mail address for the subject persons;

(2) conspicuous posting of the notice on the website of the business, if one is maintained; and

(3) notification to major statewide media.

N.C. Gen. Stat. § 75-65(e).

WHAT MUST THE NOTICE SAY?

The notice must be clear, 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 for the major consumer reporting agencies; and

(7) the toll-free numbers, addresses, and Web site addresses for the Federal Trade Commission and the North Carolina Attorney General's Office, along with a statement that the individual can obtain information from these sources about preventing identity theft.

N.C. Gen. Stat. § 75-65(d).

ARE THERE ANY EXEMPTIONS?

A financial institution that is subject to and in compliance with the Federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice, issued on March 7, 2005, by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision; or a credit union that is subject to and in compliance with the Final Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice, issued on April 14, 2005, by the National Credit Union Administration; and any revisions, additions, or substitutions relating to any of the interagency guidance, shall be deemed to be in compliance with this section. N.C. Gen. Stat. § 75-65(h).

WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

A violation of this section is a violation of N.C. Gen. Stat. § 75-1.1, which declares as unlawful any unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce. N.C. Gen. Stat. § 75-65(i). The state attorney general may seek a civil penalty up to $5,000 per violation if the violation was knowingly committedly or committed in contravention of a court order. N.C. Gen. Stat. Ann. § 75-15.2.

No private right of action exists for a violation of this section unless such individual is injured as a result of the violation. N.C. Gen. Stat. § 75-65(i). Pursuant to N.C. Gen. Stat. § 75-16, if any person is injured, or the business of any person, firm or corporation is broken up, destroyed or injured, as a result of a violation of the notification requirements, that person may seek treble damages.

ARE THERE ANY DATA SECURITY REQUIREMENTS IMPOSED?

Any business that conducts business in North Carolina and any business that maintains or otherwise possesses personal information of a resident of North Carolina must take reasonable measures to protect against unauthorized access to or use of the information in connection with or after its disposal. N.C. Gen. Stat. Ann. § 75-64(a).

The reasonable measures must include:

(1) implementing and monitoring compliance with policies and procedures that require the burning, pulverizing, or shredding of papers containing personal information so that information cannot be practicably read or reconstructed;

(2) implementing and monitoring compliance with policies and procedures that require the destruction or erasure of electronic media and other non-paper media containing personal information so that the information cannot practicably be read or reconstructed; and

(3) describing procedures relating to the adequate destruction or proper disposal of personal records as official policy in the writings of the business entity.

N.C. Gen. Stat. Ann. § 75-64(b).

A business may enter, after due diligence in the manner provided under the statute, into a written contract with, and monitor compliance by, another party engaged in the business of record destruction to destroy personal information as required by the statute. N.C. Gen. Stat. Ann. § 75-64(c).

These disposal requirements do not apply to: (1) any bank or financial institution that is subject to and in compliance with the privacy and security provision of the Gramm Leach Bliley Act; (2) any health insurer or health care facility that is subject to and in compliance with the standards for privacy of individually identifiable health information and the security standards for the protection of electronic health information of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"); or (3) any consumer reporting agency that is subject to and in compliance with the Federal Credit Reporting Act.

Damages assessed against a business because of acts or omissions of its non-managerial employees in violation of these disposal requirements shall not be trebled as provided in N.C. Gen. Stat. § 75-16 unless the business was negligent in the training, supervision, or monitoring of those employees. N.C. Gen. Stat. § 75-64(f).

ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

The North Carolina Administrative Code, tit. 4, ch. 3, sub. ch. 3M imposes an additional requirement on entities with a mortgage lender, mortgage servicer, mortgage broker, exclusive mortgage broker, or mortgage loan originator license issued pursuant to the North Carolina Secure and Fair Enforcement Mortgage Licensing Act or that subchapter. Upon a covered entity's discovery of an information security breach, the entity must within 1 business day provide to the North Carolina Banking Commission a copy of any notification which the entity is required to give under N.C. Gen. Stat. § 75-65. 4 NCAC § 3M.0402.

NORTH DAKOTA

STATUTE: N.D. Cent. Code §§ **51-30-01, *et seq*.**[84]

WHO MUST COMPLY?

Any person that owns, maintains, or licenses computerized data that includes personal information of a resident. N.D. Cent. Code §§ 51-30-02, 51-30-03.

WHAT DATA IS COVERED?

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 under N.D. Cent. Code Ann. § 39-06-14;

(3) a non-driver color photo identification card number assigned to the individual by the Department of Transportation under N.D. Cent. Code Ann § 39-06-03.1;

(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) any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional;

(8) an individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual;

(9) an identification number assigned to the individual by the individual's employer in combination with any required security code, access code, or password; or

(10) the individual's digitized or other electronic signature.

N.D. Cent. Code § 51-30-01(4)(a).

"Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. N.D. Cent. Code § 51-30-01(4)(b).

[84] Publicly available at: *Notice of Security Breach For Personal Information*, www.legis.nd.gov, **http://www.legis.nd.gov/cencode/t51c30.pdf** (last visited August 26, 2018).

Back to TOC

WHAT CONSTITUTES A DATA BREACH?

The unauthorized acquisition of computerized data when access to personal information has not been secured by encryption or by any other method or technology that renders the electronic files, media, or databases unreadable or unusable. Good-faith acquisition of personal information by an employee or agent of the person is not a breach of the security of the system, if the personal information is not used or subject to further unauthorized disclosure. N.D. Cent. Code § 51-30-01(1).

WHO MUST BE NOTIFIED?

Any resident of North Dakota whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. N.D. Cent. Code § 51-30-02.

In the event of a breach that affects more than 250 individuals, the state attorney general must be notified by mail or electronic mail. N.D. Cent. Code § 51-30-02.

Any person that maintains computerized data that includes personal information that the person does not own must 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. N.D. Cent. Code § 51-30-03.

WHEN MUST NOTICE BE SENT?

Notice to affected residents and the state attorney general must be provided 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. N.D. Cent. Code Ann. § 51-30-02.

Notice to an affected owner or licensee by a person maintaining their personal information must be provided immediately following discovery of the breach. N.D. Cent. Code § 51-30-03.

Notice may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation but must be made after the law enforcement agency determines that the notification will not compromise the investigation. N.D. Cent. Code Ann. § 51-30-04.

IN WHAT FORM AND MANNER MUST NOTICE BE SENT?

Notice under this chapter must be provided by one of the following methods:

(1) written notice;

(2) electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001; or

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

N.D. Cent. Code § 51-30-05.

Substitute notice consists of the following:

(1) electronic mail notice when the person has an electronic mail address for the subject persons;

(2) conspicuous posting of the notice on the person's website, if the person maintains one; and

(3) notification to major statewide media.

N.D. Cent. Code § 51-30-05.

WHAT MUST THE NOTICE SAY?

The statute does not address the contents of the notification.

ARE THERE ANY EXEMPTIONS?

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

A financial institution, trust company, or credit union that is subject to, examined for, and in compliance with the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice is in compliance with the statute.

A covered entity, business associate, or subcontractor subject to breach notification requirements under title 45, Code of Federal Regulations, subpart D, Part 164, is considered to be in compliance with the statute. N.D. Cent. Code § 51-30-06.

WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

A violation of this statute will be deemed a violation of N.D. Cent. Code ch. 51-15. The state attorney general has enforcement authority and possesses all powers available to it under N.D. Cent. Code ch. 51-15 and may seek all remedies provided therein. N.D. Cent. Code § 51-30-07.

The attorney general may seek an injunction, an order appointing a receiver, cease and desist order, or civil penalties up to $5,000 for each violation. N.D. Cent. Code §§ 51-15-07, 51-15-11. The attorney general is also entitled to reasonable attorney's fees, investigation fees, costs, and expenses of any investigation and action. N.D. Cent. Code § 51-30-10. The remedies, duties, prohibitions, and penalties are not exclusive and are in addition to all other causes of action, remedies, and penalties provided by law. N.D. Cent. Code Ann. § 51-30-07.

Back to TOC

ARE THERE ANY DATA SECURITY REQUIREMENTS IMPOSED?

No.

ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

None.

OHIO

STATUTE: Ohio Rev. Code §§ **1347.12**,[85] **1349.19**,[86] **1349.191**,[87] **1349.192**.[88]

WHO MUST COMPLY?

Any person that owns, licenses, maintains custody of, or stores personal information about Ohio residents. Ohio Rev. Code § 1349.19(B)(1), § 1349.19(C).

Identical notification obligations apply to any state agency or any agency of a political subdivision that owns, licenses, maintains custody of, or stores personal information about Ohio residents. Ohio Rev. Code § 1347.12. This includes any organized body, office, or agency established by the laws of Ohio or a political subdivision for the exercise of any function of state government or such political subdivision, except any "covered entities" under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). Ohio Rev. Code § 1349.19(A)(1)(a).

WHAT DATA IS COVERED?

"Personal information," meaning an individual's name, consisting of the individual's first name or first initial and last name, in combination with and linked to any one or more of the following data elements, when the data elements are not encrypted, redacted, or altered by any method or technology in such a manner that the data elements are unreadable:

(1) a social security number;

(2) a driver's license number or state identification card number; or

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

Ohio Rev. Code § 1349.19(A)(7)(a).

"Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or any of the following media that are widely distributed:

(1) any news, editorial, or advertising statement published in any bona fide newspaper, journal, or magazine, or broadcast over radio or television;

---

[85] Publicly available at: *Agency disclosure of security breach of computerized personal information data*, **http://codes.ohio.gov/**, http://codes.ohio.gov/orc/1347.12 (last visited May 30, 2019).
[86] *Private disclosure of security breach of computerized personal information data*, www.codes.ohio.gov, http://codes.ohio.gov/orc/1349.19 (last visited May 30, 2019).
[87] Publicly available at: *Investigation of noncompliance with disclosure laws*, www.codes.ohio.gov, **http://codes.ohio.gov/orc/1349.191** (last visited May 30, 2019).
[88] Publicly available at: *Civil action by attorney general for violation of disclosure laws*, www.codes.ohio.gov, **http://codes.ohio.gov/orc/1349.192** (last visited May 30, 2019).

(2) any gathering or furnishing of information or news by any bona fide reporter, correspondent, or news bureau to news media described in (1);

(3) any publication designed for and distributed to members of any bona fide association or charitable or fraternal nonprofit corporation; or

(4) any type of media similar in nature to any item, entity, or activity identified in (1)-(3).

Ohio Rev. Code § 1349.19(A)(7)(b).

"Encrypted" means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key. Ohio Rev. Code § 1349.19(A)(4).

"Redacted" means altered or truncated so that no more than the last four digits of a social security number, driver's license number, state identification card number, account number, or credit or debit card number is accessible as part of the data. Ohio Rev. Code § 1349.19(A)(9).

WHAT CONSTITUTES A DATA BREACH?

The unauthorized access to and acquisition of computerized data that compromises the security or confidentiality of personal information owned or licensed by a person and that causes, reasonably is believed to have caused, or reasonably is believed will cause a material risk of identity theft or other fraud to the person or property of a resident of the state. Ohio Rev. Code § 1349.19(A)(1)(a).

Good faith acquisition of personal information by an employee or agent of the person for the purposes of the person is not a breach of the security of the system, provided that the personal information is not used for an unlawful purpose or subject to further unauthorized disclosure. Ohio Rev. Code § 1349.19(A)(1)(b)(i).

WHO MUST BE NOTIFIED?

Any resident of Ohio whose personal information was, or reasonably is believed to have been, accessed and acquired by an unauthorized person if the access and acquisition by the unauthorized person causes or reasonably is believed will cause a material risk of identity theft or other fraud to the resident. A "resident" is an individual whose principal mailing address as reflected in the records of the person is in Ohio. Ohio Rev. Code § 1349.19(B)(1).

If circumstances require disclosure to more than 1,000 residents involved in a single occurrence of a breach, the person must notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution, and content of the disclosure given by the person to affected residents. A person may not delay making any required disclosure or notification in order to make this notification. Ohio Rev. Code § 1349.19(G).

Any person that is the custodian of or stores computerized data that includes personal information on behalf of another person must notify the other person of a breach 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 reasonably is believed will cause a material risk of identity theft or other fraud to a resident of this state. Ohio Rev. Code § 1349.19(C).

WHEN MUST NOTICE BE SENT?

Notice to affected residents must be provided 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 activities and consistent with any measures necessary to determine the scope of the breach, including which residents' personal information was accessed and acquired, and to restore the reasonable integrity of the data system. Ohio Rev. Code Ann. § 1349.19(B)(2).

Notice to affected persons by a person with custody of or storing their personal information must be provided in an expeditious manner. Ohio Rev. Code § 1349.19(C).

Notification may be delayed if a law enforcement agency determines that the disclosure or notification will impede a criminal investigation or jeopardize homeland or national security, in which case, the person must make the disclosure or notification after the law enforcement agency determines that disclosure or notification will not compromise the investigation or jeopardize homeland or national security. Ohio Rev. Code § 1349.19(D).

IN WHAT FORM AND MANNER MUST NOTICE BE SENT?

Any of the following methods:

(1) written notice;

(2) electronic notice, if that was the primary method of communication with the resident;

(3) telephone notice; or

(4) substitute notice, if the person required to provide notice demonstrates they do not have sufficient contact information to provide notice using the above methods, or that the cost of providing the required notice to residents would exceed $250,000, or that the affected class of subject residents requiring notice exceeds 500,000 persons.

Ohio Rev. Code § 1349.19(E)(1)-(3).

Substitute notice shall consist of all of the following:

(a) Electronic mail notice if the person has an electronic mail address for the resident to whom the disclosure must be made;

(b) Conspicuous posting of the disclosure or notice on the person's website, if the person maintains one; and

(c) Notification to major media outlets, to the extent that the cumulative total of the readership, viewing audience, or listening audience of all of the outlets so notified equals or exceeds 75% of the population of Ohio. Ohio Rev. Code §§ 1347.12(E)(4); 1349.19(E)(4).

If the person demonstrates that they are a business entity with 10 or fewer employees and the cost of providing the required notice to residents will exceed $10,000, substitute notice may be provided by doing all of the following:

(1) Notification by a paid advertisement in a local newspaper that is distributed in the geographic area in which the person is located, which advertisement shall be of sufficient size that it covers at least one-quarter of a page in the newspaper and shall be published in the newspaper at least once a week for three consecutive weeks;

(2) Conspicuous posting of the disclosure or notice on the person's website, if one is maintained; and

(3) Notification to major media outlets in the geographic area in which the person is located.

Ohio Rev. Code § 1349.19(E)(5).
The required notification may be made pursuant to any provision of a contract entered into by the person with another person prior to the date of the breach if that contract does not conflict with or waive any provision of the statute. Ohio Rev. Code § 1349.19(B)(1).

WHAT MUST THE NOTICE SAY?

The statute does not specify the contents of the notification.

ARE THERE ANY EXEMPTIONS?

A financial institution, trust company, or credit union or any affiliate thereof that is required by federal law, including, but not limited to, any federal statute, regulation, regulatory guidance, or other regulatory action, to notify its customers of an information security breach with respect to information about those customers and that is subject to examination by its functional government regulatory agency for compliance with the applicable federal law, is exempt from the requirements of this statute. Ohio Rev. Code § 1349.19(F)(1).

In addition, the statute does not apply to any "covered entities" under HIPAA. Ohio Rev. Code § 1349.19(F)(2).

Acquisition of personal information pursuant to a search warrant, subpoena, or court/regulatory agency order is not a breach. Ohio Rev. Code § 1349.19(A)(1)(b)(ii).

WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

The state attorney general may conduct an investigation and may bring a civil action upon an alleged failure to comply with the requirements of the statute. Ohio Rev. Code §§ 1349.12(G), 1349.19(I). The state attorney general has exclusive authority to enforce this statute. Ohio Rev. Code Ann. § 1349.192(A)(1).

The state attorney general may seek a temporary restraining order, preliminary or permanent injunction, and civil penalties as follows:

(1) $1,000 for each day a person has intentionally or recklessly failed to comply with the statute;

(2) $5,000 for each day after 60 days and up to 90 days that a person has intentionally or recklessly failed to comply with the statute;

(3) $10,000 for each day after 90 days that a person has intentionally or recklessly failed to comply with the statute; and

(4) if the person intentionally or reckless failed to comply with the statute for more than 90 days, $1,000 for each day of the first 60 days of non-compliance, $5,000 for each day of the 61st through 90th days of non-compliance, and $10,000 for each day of non-compliance thereafter.

Ohio Rev. Code § 1349.192(A)(1).

The attorney general may seek the costs of conducting an investigation and bringing an action. Ohio Rev. Code § 1349.192(B).

ARE THEREN ANY DATA SECURITY REQUIREMENTS IMPOSED?

No.

ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

Yes.

Insurance:

Under Bulletin 2009-12 issued by the Ohio Department of Insurance, any person or entity holding a license or certificate of authority from the Superintendent of Insurance to conduct business in Ohio is required to notify the Superintendent of any Loss of Control, as defined below, of policyholder information in their possession within 15 calendar days of discovery of such Loss of Control. Such notification is required when an incident involves the loss of personal information of more than 250 Ohio residents.

“Loss of Control” means the unauthorized access to, unauthorized acquisition of, or disappearance of any personal information, including with respect to computerized data, the

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

For purposes of this bulletin, "personal information" means an individual's name, consisting of the individual's first name or first initial and last name, in combination with a: (1) social security number, (2) driver's license or state identification number, or (3) bank/credit/debit card or account number.

In addition, under Chapter 3965: Cybersecurity Requirements for Insurance Companies,[89] if a licensee learns that a cybersecurity event has or may have occurred, the licensee or an outside vendor or service provider designated to act on behalf of the licensee shall conduct a prompt investigation. During the investigation, the licensee or an outside vendor or service provider designated to act on behalf of the licensee shall, at a minimum, do as much as determine whether a cybersecurity event has occurred, assess the nature and scope of the cybersecurity event, identify any nonpublic information that may have been involved in the cybersecurity event, and perform or oversee reasonable measures to restore the security of the information systems compromised in the cybersecurity event in order to prevent further unauthorized acquisition, release, or use of nonpublic information in the licensee's possession, custody, or control. Ohio Rev. Code §3965.03.

Further, each licensee shall notify the superintendent of insurance as promptly as possible after a determination that a cybersecurity event involving nonpublic information in the possession of the licensee has occurred, but in no event later than three business days. Ohio Rev. Code §3965.04.

Finally, the superintendent of insurance shall have power to examine and investigate into the affairs of any licensee to determine whether the licensee has been or is engaged in any conduct in violation of the law. Whenever the superintendent has reason to believe that a licensee has been or is engaged in conduct in Ohio that violates the law, the superintendent may take any necessary or appropriate action to enforce the provisions of this chapter. Ohio Rev. Code §3965.05.

[89] Publicly available at: *Cybersecurity Requirements for Insurance Companies*, www.codes.ohio.gov**,** http://codes.ohio.gov/orc/3965 (last visited May 30, 2019).

Back to TOC

OKLAHOMA

STATUTE: Okl. Stat. 74 § 3113.1,[90] 24 § 161-166.[91]

WHO MUST COMPLY?

Any individual or entity that owns, licenses, or maintains computerized data that includes personal information regarding any resident of Oklahoma. Okl. Stat. 74 § 3113.1(A), 24 §162.

WHAT DATA IS COVERED?

First name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of the State, when the data elements are neither encrypted nor redacted:

(1) social security number;

(2) driver license number or state identification card number issued in lieu of a driver license; or

(3) financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to the financial accounts of a resident. Okl. Stat. 74 § 3113.1(D)(2); Okl. Stat. 24 § 162(6).

The statute does not apply if affected data is encrypted or redacted. Okl. Stat. 24 § 162(6). "Encrypted" means transformation of data through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key, or securing the information by another method that renders the data elements unreadable or unusable. Okl. Stat. 24 § 162(3).

"Redact" means alteration or truncation of data such that no more than the following are accessible as part of the personal information:

(1) five digits of a social security number; or

(2) the last four digits of a driver license number, state identification card number or account number. Okl. Stat. 24 § 162(8).

The statute does not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public. Okl. Stat. 24 § 162(6).

[90] Publicly available at: *Oklahoma State Court Network*, http://www.oscn.net, http://www.oscn.net/applications/oscn/DeliverDocument.asp?CiteID=447784 (last visited May 30, 2019).
[91] Publicly available at: *Oklahoma State Court Network*, http://www.oscn.net, https://www.oscn.net/applications/oscn/DeliverDocument.asp?CiteID=452235 (last visited May 30, 2019).

WHAT CONSTITUTES A DATA BREACH?

The unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes, or the individual or entity reasonably believes has caused or will cause, identity theft or other fraud to any resident of the State. Okla. Stat. 24 § 162(1).

The good faith acquisition of personal information by an employee or agent of an individual or entity for the purposes of the individual or the entity is not a breach of the security of the system, provided that the personal information is not used for a purpose other than a lawful purpose of the individual or entity or subject to further unauthorized disclosure. Okla. Stat. 24 § 162(1).

WHO MUST BE NOTIFIED?

Any resident of the State whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person and that causes, or the individual or entity reasonably believes has caused or will cause, identity theft or other fraud to any resident of the State. Okla. Stat. 74 §§ 3113.1(A), (B).

An individual or entity that maintains covered computerized data must notify the owner or licensee of that information. Okla. Stat. 24 § 163(C).

WHEN MUST NOTICE BE SENT?

Notice must be sent upon discovery of the breach without unreasonable delay, subject to law enforcement and investigative needs. In the case of breaches affecting data held by a person on behalf of another entity, notice must be sent as soon as practicable following discovery. Okla. Stat. 24 § 163(b),(c).

IN WHAT FORM AND MANNER MUST NOTICE BE SENT?

Notice must be sent in one of the following ways:

(1) written notice to the postal address in the records of the individual or entity;

(2) telephone notice;

(3) electronic notice; or

(4) substitute notice, if the individual or the entity required to provide notice demonstrates that the cost of providing notice will exceed $50,000, or that the affected class of residents to be notified exceeds 100,000 persons, or that the individual or the entity does not have sufficient contact information or consent to provide notice as described in (1), (2) or (3) above. Okla. Stat. 24 § 162(7).

Substitute notice consists of any two of the following:

(1) email notice if the individual or the entity has email addresses for the members of the affected class of residents;

(2) conspicuous posting of the notice on the Internet web site of the individual or the entity if the individual or the entity maintains a public Internet web site;

(3) notice to major statewide media. Okla. Stat. 24 § 162(7).

WHAT MUST THE NOTICE SAY?

The statute does not specify the contents of the notification.

ARE THERE ANY EXEMPTIONS?

Yes:

an entity that maintains its own notification procedures as part of an information privacy or security policy for the treatment of personal information and that are consistent with the timing requirements of the act shall be deemed to be in compliance with the notification requirements of the act if it notifies residents of the State in accordance with its procedures in the event of a breach of security of the system; and

a financial institution that complies with the notification requirements prescribed by the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice is deemed to be in compliance with the provisions of the act. Okla. Stat. 24 § 164.

WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

A violation of the act that results in injury or loss to residents of the 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.

Except as provided for in the next paragraph, the Attorney General or a district attorney shall have exclusive authority to bring action and may obtain either actual damages for a violation of the act 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 of the act by a State-chartered or State-licensed financial institution shall be enforceable exclusively by the primary State regulator of the financial institution. Okla. Stat. 24 § 165.

ARE THERE ANY DATA SECURITY REQUIREMENTS IMPOSED?

No.

ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

None.

OREGON

STATUTE: Or. Rev. Stat. §§ **646A.600-628**[92]

WHO MUST COMPLY?

A 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 and that was subject to a breach of security or a person who received notice of a breach of security from another person that maintains or otherwise possesses personal information on the person's behalf; or a person that maintains or otherwise possesses personal information on behalf of another person. Or. Rev. Stat. §§ 646a.604(1), (2).

WHAT DATA IS COVERED?

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

(1) a consumer's social security number;

(2) a consumer's driver license number or state identification card number issued by the Department of Transportation;

(3) a consumer's passport number or other identification number issued by the United States;

(4) a consumer's 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;

(5) data from automatic 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;

(6) 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; and

(7) any information about a consumer's medical history or mental or physical condition or about a health care professional's medical diagnosis or treatment of the consumer. Or. Rev. Stat. § 646A.602(11)(a).

[92] Publicly available at: **https://www.oregonlegislature.gov/bills_laws/ors/ors646a.html** (last visited May 30, 2019).

The statute does not apply if the data is encrypted unless the breach involves encrypted data and the encryption key has been compromised. Or. Rev. Stat. § 646A.602(11)(a). "Encryption" means an algorithmic process that renders data unreadable or unusable without the use of a confidential process or key. Or. Rev. Stat. § 646A.602(6).

WHAT CONSTITUTES A DATA BREACH?

The unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information that a person maintains. Or. Rev. Stat. § 646A.602(1)(a).

The statute does not apply to an inadvertent acquisition of personal information by a person or the person's employee or agent if the personal information is not used in violation of applicable law or in a manner that harms or poses an actual threat to the security, confidentiality or integrity of the personal information. Or. Rev. Stat. § 646A.602(1)(b).

WHO MUST BE NOTIFIED?

The consumer to whom the personal information pertains. Or. Rev. Stat. § 646A.604(1)(a)

The Attorney General must be notified if the breach affects more than 250 residents. Or. Rev. Stat. § 646A.604(1)(b).

Consumer report agencies (CRAs) must be notified whenever a breach affects more than 1,000 residents. Or. Rev. Stat. § 646A.604(6).

A person that maintains or otherwise possesses personal information on behalf of another person shall notify the other person after discovering a breach of security. Or. Rev. Stat. § 646A.604(2).

WHEN MUST NOTICE BE SENT?

The notice must be sent in the most expeditious manner possible, and without unreasonable delay, but not later than forty-five (45) days after discovering or receiving notification of the breach of security. Or. Rev. Stat. § 646A.604(1)(a),(2).

IN WHAT FORM AND MANNER MUST NOTICE BE SENT?

Notification must be provided by one of the following methods:

(1) in writing;

(2) electronically, if the person customarily communicates with the consumer electronically;

(3) by telephone, if the person contacts the affected consumer directly; or

(4) with substitute notice, if the person demonstrates that the cost of notification otherwise would exceed $250,000, or that the affected class of consumers exceeds

350,000, or if the person does not have sufficient contact information to notify affected consumers.

Substitute notice consists of the following:

(1) posting the notice or a link to the notice conspicuously on the home page of the person's website if the person maintains a website; and

(2) notifying major statewide television and newspaper media. Or. Rev. Stat. § 646A.604(4).

WHAT MUST THE NOTICE SAY?

Notice must include, at a minimum, the following:

(1) a description of the breach of security in general terms;

(2) the approximate date of the breach of security;

(3) the type of personal information that was subject to the breach of security;

(4) contact information for the person that gave notice;

(5) contact information for national consumer reporting agencies; and

(6) advice to the consumer to report suspected identity theft to law enforcement, including the Attorney General and the Federal Trade Commission. Or. Rev. Stat. § 646A.604(5).

ARE THERE ANY EXEMPTIONS?

A person does not need to notify consumers of a breach of security if, after an appropriate investigation or after consultation with relevant federal, state or local law enforcement agencies, the person reasonably determines that the consumers whose personal information was subject to the breach of security are unlikely to suffer harm. Or. Rev. Stat. § 646A.604(8).

Covered entities under the Health Insurance Portability and Accountability Act ("HIPAA") are exempted from compliance, so long as a copy of the notice sent to either the entity's primary functional regulator or to State residents is also sent to the Attorney General. Or. Rev. Stat. § 646A.604(9).

In addition, a person that is subject to and complies with regulations promulgated pursuant to Title V of the Gramm-Leach-Bliley Act of 1999 (15 U.S.C.§§ 6801 to 6809), as that Act existed on January 1, 2016, is exempt from the statute. Or. Rev. Stat. § 646A.604(9)(c).

WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

If the Director of the Department of Consumer and Business Services has reason to believe that any person has engaged or is engaging in any violation of §§ 646A.600 to 646A.628, the

Director may issue an order, subject to chapter 183, directed to the person to cease and desist from the violation, or require the person to pay compensation to consumers injured by the violation. The Director may order compensation to consumers only upon a finding that enforcement of the rights of the consumers by private civil action would be so burdensome or expensive as to be impractical. In addition, any person who violates or who procures, aids or abets in the violation of §§ 646A.600 to 646A.628 shall be subject to a penalty of not more than $1,000 for every violation. Every violation is a separate offense and, in the case of a continuing violation, each day's continuance is a separate violation, but the maximum penalty for any occurrence shall not exceed $500,000. Civil penalties under the statute shall be imposed as provided in § 183.745. Or. Rev. Stat. § 646A.624.

ARE THERE ANY DATA SECURITY REQUIREMENTS IMPOSED?

A person that owns, maintains, or otherwise possesses, or has control over or access to, data that includes personal information must implement an information security program that includes:

(1) Administrative safeguards such as:

(1) Designating one or more employees to coordinate the security program;

(2) Identifying reasonably foreseeable internal and external risks with reasonable regularity;

(3) Assessing whether existing safeguards adequately control the identified risks;

(4) Training and managing employees in security program practices and procedures with reasonable regularity;

(5) Selecting service providers that are capable of maintaining appropriate safeguards and practices, and requiring the service providers by contract to maintain the safeguards and practices; and

(6) Adjusting the security program in light of business changes, potential threats or new circumstances; and

(7) Reviewing user access privileges with reasonable regularity;

(2) Technical safeguards such as:

(1) Assessing risks and vulnerabilities in network and software design and taking reasonably timely action to address the risks and vulnerabilities;

(2) Assessing risks in information processing, transmission and storage;

(3) Applying security updates and a reasonable security patch management program to software that might reasonably be at risk of or vulnerable to a breach of security;

(4) Monitoring, detecting, preventing and responding to attacks or system failures; and

(5) Regularly testing, monitoring and taking action to address the effectiveness of key controls, systems and procedures; and

(3) Physical safeguards such as:

(1) Assessing, in light of current technology, risks of information collection, storage, usage, retention, access and disposal and implementing reasonable methods to remedy or mitigate identified risks;

(2) Monitoring, detecting, preventing, isolating and responding to intrusions timely and with reasonable regularity;

(3) Protecting against unauthorized access to or use of personal information during or after collecting, using, storing, transporting, retaining, destroying or disposing of the personal information; and

(4) Disposing of personal information, whether the person disposes of the personal information on or off the person's premises or property, after the person no longer needs the personal information for business purposes or as required by local, state or federal law by burning, pulverizing, shredding or modifying a physical record and by destroying or erasing electronic media so that the information cannot be read or reconstructed. Or. Rev. Stat. § 646A.622.

ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

None.

PENNSYLVANIA

STATUTE: 73 Pa. Stat. § **2301** *et seq.*[93]

WHO MUST COMPLY?

Any entity that maintains, stores, or manages computerized data that includes personal information regarding a Pennsylvania resident. 73 Pa. Stat. § 2303(a).

A vendor that maintains, stores, or manages computerized data on behalf of another entity. 73 Pa. Stat. § 2303(c).

WHAT DATA IS COVERED?

Covered information includes a Pennsylvania resident's first name or first initial and last name, plus: (1) social security number; (2) driver's license or state identification card number; or (3) financial account, credit card or debit card number in combination with any required security or access code or password that would permit access to a resident's financial account. 73 Pa. Stat. § 2302.

The statute does not apply to information that is encrypted or redacted, so long as the encryption key was not accessed or acquired. 73 Pa. Stat. § 2303(b).

WHAT CONSTITUTES A DATA BREACH?

The unauthorized access and acquisition that materially compromises the security or confidentiality of a database of covered information and that causes, has caused, will cause loss or injury to any resident of Pennsylvania, excluding certain good-faith acquisitions by employees or agents. 73 Pa. Stat. § 2302.

WHO MUST BE NOTIFIED?

Any resident of Pennsylvania whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person. 73 Pa. Stat. § 2303(a).

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. 73 Pa. Stat. § 2303(c).

If more than 1,000 persons are notified, all nationwide CRAs must be notified without unreasonable delay of timing. 73 Pa. Stat. § 2305.

WHEN MUST NOTICE BE SENT?

[93] Publicly available at: *Breach of Personal Information Notification Act*, https://codes.findlaw.com/pa/title-73-ps-trade-and-commerce/#!tid=N9B3F41908C4F11DA86FC8D90DD1949D4 (last visited June 06, 2019).

Notification must be made without unreasonable delay taking any necessary measures to determine the scope of the breach and to reasonably restore the integrity of the system. Notification may be delayed if law enforcement determines and advises the covered entity in writing that notification will impede a criminal or civil investigation. 73 Pa. Stat. § 2303(a).[94],73 Pa. Stat. § 2303(c), 73 Pa. Stat. § 2304.

IN WHAT FORM AND MANNER MUST NOTICE BE SENT?

Notice must be provided by any of the following methods:

(1) written notice to the last known home address for the individual;

(2) telephonic notice, if the customer can be reasonably expected to receive it and the notice is given in a clear and conspicuous manner, describes the incident in general terms and verifies personal information but does not require the customer to provide personal information, and the customer is provided with a telephone number to call or provided with an Internet website to visit for further information or assistance;

(3) email notice, if a prior business relationship exists and the person or entity has a valid email address for the individual; or

(4) Substitute notice, if the entity demonstrates one of the following:

(a) the cost of providing notice would exceed $100,000;

(b) the affected class of subject persons to be notified exceeds 175,000; or

(c) the entity does not have sufficient contact information.

(d) Substitute notice shall consist of all of the following:

(e) email notice when the entity has an email address for the subject persons;

(f) conspicuous posting of the notice on the entity's Internet website if the entity maintains one; and

(g) notification to major Statewide media. § 2302 (definition of "Notice").

WHAT MUST THE NOTICE SAY?

Notice must be clear and conspicuous, describe the incident in general terms, verify the covered information (the consumer is not required to provide the covered information to the entity), and

[94] 2017 PA H.B. 1846: proposal to make notification within 45 days of discovery of the breach; to require vendor notification; to require state agencies, counties, school districts, or municipalities to provide special notice.

provide a telephone number or website for further information or assistance. 73 Pa. Stat. § 2302.[95]

ARE THERE ANY EXEMPTIONS?

Yes. An entity that maintains its own notification procedures as part of an information privacy or security policy for the treatment of personal information which is consistent with the notice requirements of the statute shall be deemed to be in compliance with the notification requirements of the statute if it notifies subject persons in accordance with its policies in the event of a breach of security of the system. 73 Pa. Stat. § 2307(a).

In addition, a financial institution that complies with the notification requirements prescribed by the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice is deemed to be in compliance with the statute. 73 Pa. Stat. § 2307(b).

Further, an entity that complies with the notification requirements or procedures pursuant to the rules, regulations, procedures or guidelines established by the entity's primary or functional federal regulator shall be in compliance with the statute. 73 Pa. Stat. § 2307(b).

WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

The Office of the Attorney General shall have exclusive authority to bring an action under the Unfair Trade Practices and Consumer Protection Law for a violation of this Act. 73 Pa. Stat. § 2308. Private rights of action are not permitted. No other penalties are specified in the statute.

ARE THERE ANY DATA SECURITY REQUIREMENTS IMPOSED?

No.

ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

None.[96]

[95] 2017 PA H.B. 1548 (NS): proposal to require additional specific and lengthy mandatory content for notice and mandatory format.

[96] 2017 PA H.B. 1548 (NS): proposal to require notification by specific entities including state agencies, political subdivisions of the Commonwealth, and individuals or businesses doing business in the Commonwealth.

PUERTO RICO

STATUTE: 10 P.R. Laws Ann. § **4051** ***et seq.***[97]

WHO MUST COMPLY?

Any entity that is the owner or custodian of a database that includes personal information of residents of Puerto Rico. 10 P.R. Laws Ann. § 4052.

WHAT DATA IS COVERED?

Protected information refers to at least the name or first initial and the surname of a person, together with any of the following data so that an association may be established between certain information with another and in which the information is legible enough so that in order to access it there is no need to use a special cryptographic code:

(1) social security number;

(2) driver 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 Health Insurance Portability and Accountability Act ("HIPAA");

(6) tax information; or

(7) work-related evaluations. 10 P.R. Laws Ann.§ 4051(a).

Neither the mailing nor the residential address is included in the protected information or information that is a public document and that is available to the citizens in general. 10 P.R. Laws Ann.§ 4051(a).

WHAT CONSTITUTES A DATA BREACH?

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; or when normally authorized persons or entities have had access and it is known or there is reasonable suspicion that they have violated the professional confidentiality or obtained authorization under false representation with the intention of making illegal use of the information. This includes both access to the data banks through the system and

[97] Publicly available at: **https://www.dwt.com/files/Uploads/Documents/Publications/PuertoRico%20Security%20Breach.pdf**.

physical access to the recording media that contain the same and any removal or undue retrieval of the recordings. 10 P.R. Laws Ann.§ 4051(c).

WHO MUST BE NOTIFIED?

Any citizen of Puerto Rico whose personal information has been subject to a security violation. 10 P.R. Laws Ann.§ 4052.

WHEN MUST NOTICE BE SENT?

Notice must be sent as expeditiously as possible, taking into consideration the need of law enforcement agencies to secure possible crime scenes and evidence as well as the application of measures needed to restore the system's security. 10 P.R. Laws Ann.§ 4052.

Within a non-extendable term of 10 days after the violation of the system's security has been detected, the parties responsible shall inform the Department of Consumer Affairs, which shall make a public announcement of the fact within 24 hours after having received the information. 10 P.R. Laws Ann.§ 4052.

IN WHAT FORM AND MANNER MUST NOTICE BE SENT?

Notice must be provided by one of the following methods:

(1) written notice; or

(2) authenticated electronic means according to the Digital Signatures Act. 10 P.R. Laws Ann.§ 4053(1).

When the cost of notifying all those potentially affected or of identifying them is excessively onerous due to the number of persons affected, or due to the difficulty in locating all persons, or due to the economic situation of the enterprise or entity, or whenever the cost exceeds $100,000 or the number of persons exceeds 100,000, the entity shall issue the notice through the following two steps:

(1) prominent display of an announcement to that respect at the entity's premises, on the web page of the entity, if any, and in any informative flier published and sent through mailing lists both postal and electronic; and

(2) a communication to that respect to the media informing of the situation and providing information as to how to contact the entity to allow for better follow-up. When the information is of relevance to a specific professional or commercial sector, the announcement may be made through publications or programming of greater circulation oriented towards that sector. 10 P.R. Laws Ann.§ 4053(2).

WHAT MUST THE NOTICE SAY?

The notice of the security system breach shall be submitted in a clear and conspicuous manner and should describe the breach in general terms and the type of sensitive information

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. 10 P.R. Laws Ann.§ 4053.

ARE THERE ANY EXEMPTIONS?

None.

WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

The Secretary of State may impose fines of $500 up to a maximum of $5,000 for each violation. Private rights of action are allowed. The fines imposed by the Secretary of State do not affect the rights of the consumers to initiate actions or claims for damages before a competent court. 10 P.R. Laws Ann.§ 4055.

ARE THERE ANY DATA SECURITY REQUIREMENTS IMPOSED?

No.

ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

In those cases in which the breach or irregularity in the security systems of the database occurs in a government agency or public corporation, it shall be notified to the Citizen's Advocate Office, which shall assume jurisdiction. For this purpose, the Citizen’s Advocate shall designate a Specialized Advocate who shall address these types of cases. 10 L.P.R.A. § 4054a.

RHODE ISLAND

STATUTE: 11 R.I. Gen. Laws § **49.3-1** ***et seq.***[98]

Any State agency or person that owns, maintains or licenses computerized data that includes personal information. 11 R.I. Gen. Laws § 49.3-4(a)(1).

For purposes of this section, personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. R.I. Gen. Laws § 11-49.3-3(b).

WHAT DATA IS COVERED?

Individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(1) social security number;

(2) driver's license number or Rhode Island Identification Card number; or

(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. 11 R.I. Gen. Laws § 49.3-3(a)(8).

The statute does not apply if the compromised data was encrypted. "Encrypted" means the transformation of data through the use of a 128 bit or higher algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key. Data shall not be considered to be encrypted if it is acquired in combination with any key, security code, or password that would permit access to the encrypted data. 11 R.I. Gen. Laws § 49.3-3(a)(1),(2).

WHAT CONSTITUTES A DATA BREACH?

The unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the State agency or person. 11 R.I. Gen. Laws § 49.3-3(1).

A breach, however, does not include good faith acquisition of the information. 11 R.I. Gen. Laws § 49.3-3(a)(1).

WHO MUST BE NOTIFIED?

Any resident of Rhode Island whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person or entity and there is a significant risk of identity theft. 11 R.I. Gen. Laws § 49.3-4(a)(1).

[98] Publicly available at: *Identify Theft Protection Act of 2015*, www.rilin.state.ri.us, **http://webserver.rilin.state.ri.us/Statutes/title11/11-49.3/INDEX.HTM** (last visited June 06, 2019).

If more than 500 Rhode Island residents are to be notified, the municipal agency, State agency, or person shall notify 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. Notification to the Attorney General and the major credit reporting agencies shall be made without delaying notice to affected Rhode Island residents. 11 R.I. Gen. Laws § 49.3-4(a)(2).

WHEN MUST NOTICE BE SENT?

Notice must be made in the most expedient time possible, but no later than 45 calendar days after confirmation of the breach and the ability to ascertain the information required to fulfill the statute's notice requirements 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.11 R.I. Gen. Laws § 49.3-4(a)(2).

In the event notice must be given to the Attorney General and major credit reporting agencies, notification shall be made without delaying notice to affected Rhode Island residents. 11 R.I. Gen. Laws § 49.3-4(a)(2).

Notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification shall be made after the law enforcement agency determines that it will not compromise the investigation. 11 R.I. Gen. Laws § 49.3-4(b).

IN WHAT FORM AND MANNER MUST NOTICE BE SENT?

Notice must be provided by one of the following methods:

(1) written notice;

(2) electronic notice; or

(3) substitute notice, if the State agency or person demonstrates that the cost of providing notice would exceed $25,000, or that the affected class of subject persons to be notified exceeds 50,000, or the State agency or person does not have sufficient contact information.

Substitute notice shall consist of all of the following:

(1) email notice when the State agency or person has an email address for the subject persons;

(2) conspicuous posting of the notice on the State agency's or person's website page, if the State agency or person maintains one; and

(3) notification to major statewide media. 11 R.I. Gen. Laws § 49.3-3(c).

WHAT MUST THE NOTICE SAY?

The notification to individuals must include the following information to the extent known:

(1) a general and brief description of the incident, including how the security breach occurred and the number of affected individuals;

(2) the type of information that was subject to the breach;

(3) the date of breach, estimated date of breach, or the date range within which the breach occurred;

(4) the date that the breach was discovered;

(5) a clear and concise description of any remediation services offered to affected individuals, including toll free numbers and websites to contact for the following:

(a) credit reporting agencies;

(b) remediation service providers; and

(c) the Attorney General; and

(d) a clear and concise description of the consumer's ability to file or obtain a police report; how a consumer can request a security freeze and the necessary information to be provided when requesting the security freeze; and that fees may be required to be paid to the consumer reporting agency. 11 R.I. Gen. Laws § 49.3-4(d).

ARE THERE ANY EXEMPTIONS?

A financial institution, trust company, credit union, or its affiliates that is subject to and examined for, and found in compliance with, the Federal Interagency Guidelines on Response Programs for Unauthorized Access to Customer Information and Customer Notice shall be deemed in compliance with this chapter. 11 R.I. Gen. Laws § 49.3-6(b).

In addition, a provider of health care, health care service plan, health insurer, or a covered entity governed by the medical privacy and security rules issued by the Federal Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") shall be deemed in compliance with this chapter. 11 R.I. Gen. Laws § 49.3-6(c).

WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

Whenever the Attorney General has reason to believe that a violation of this chapter has occurred and that proceedings would be in the public interest, the Attorney General may bring an action in the name of the State against the business or person in violation. 11 R.I. Gen. Laws § 49.3-5(c).

Each reckless violation of this chapter is a civil violation for which a penalty of not more than $100 per record may be adjudged against a defendant. 11 R.I. Gen. Laws § 49.3-5(a).

Each knowing and willful violation of this chapter is a civil violation for which a penalty of not more than $200 per record may be adjudged against a defendant. 11 R.I. Gen. Laws § 49.3-5(b).

ARE THERE ANY DATA SECURITY REQUIREMENTS IMPOSED?

No.

ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

Pursuant to Rhode Island Insurance Regulation 107, licensees of the Rhode Island Department of Business Regulation, which includes insurance companies and producers, must notify the Department of a breach of the security of computerized unencrypted data that poses a significant risk of identity theft. The disclosure to the Department is required to be made in the most expedient time possible and without unreasonable delay consistent with the disclosure required in State's data breach notification law. 11 R.I. ADC § 5.107:11.

Any person that that stores, collects, processes, maintains, acquires, uses, owns or licenses personal information about a Rhode Island resident shall implement and maintain a risk-based information security program that contains reasonable security procedures and practices appropriate to the size and scope of the organization; the nature of the information; and the purpose for which the information was collected in order to protect the personal information from unauthorized access, use, modification, destruction, or disclosure and to preserve the confidentiality, integrity, and availability of such information. 11 R.I. Gen. Laws § 49.3-2(a).

SOUTH CAROLINA

STATUTE: S.C. Code § **39-1-90**[99]

WHO MUST COMPLY?

A person conducting business in South Carolina and owning, maintaining, or licensing computerized data or other data that includes personal identifying information of a South Carolina resident. S.C. Code § 39-1-90(A), (B).

WHAT DATA IS COVERED?

The first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of the State, when the data elements are neither encrypted nor redacted and is not otherwise publicly available:

(1) social security number;

(2) driver's license number or state identification card number issued instead of a driver's license;

(3) financial account number, or credit card or debit card number in combination with any required security code, access code, or password that would permit access to a resident's financial account; or

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

Personal Identifying information does not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the greater public. S.C. Code § 39-1-90(D)(3).

WHAT CONSTITUTES A DATA BREACH?

The unauthorized access to and acquisition of computerized data that was not rendered unusable through encryption, redaction, or other methods that compromises the security, confidentiality, or integrity of personal identifying information maintained by the person, when illegal use of the information has occurred or is reasonably likely to occur or use of the information creates a material risk of harm to a resident. Breach does not include the good faith acquisition of the information as defined by the statute. S.C. Code § 39-1-90(D)(1).

[99] Publicly available at: *South Carolina Legislature*, www.scstatehouse.gov, **http://www.scstatehouse.gov/code/t39c001.php** (last visited June 10, 2019).

WHO MUST BE NOTIFIED?

Any resident of South Carolina whose personal information was affected. S.C. Code § 39-1-90(A). If the breach affected data held by a third-party vendor, that vendor must notify the owner or licensor of that data. S.C. Code § 39-1-90(B).

Notification is also required to be made to the Consumer Protection Division of the Department of Consumer Affairs and all nationwide consumer reporting agencies if the breach affects more than 1,000 people. S.C. Code § 39-1-90(K).

WHEN MUST NOTICE BE SENT?

The disclosure must be made 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. The notification required by the statute may be delayed if a law enforcement agency determines that the notification impedes a criminal investigation. The notification required by the statute must be made after the law enforcement agency determines that it no longer compromises the investigation. S.C. Code § 39-1-90(A)(C).

A person conducting business in the State and maintaining computerized data or other data that includes personal identifying information that the person does not own shall notify the owner or licensee of the information of a breach of the security of the data immediately following discovery, if the personal identifying information was, or is reasonably believed to have been, acquired by an unauthorized person. S.C. Code § 39-1-90(B).

IN WHAT FORM AND MANNER MUST NOTICE BE SENT?

Notice must be provided by one of the following methods:

(1) written notice;

(2) electronic notice (consistent with the requirements of the statute);

(3) telephonic notice; or

(4) substitute notice, if the person demonstrates that the cost of providing notice exceeds $250,000, or that the affected class of subject persons to be notified exceeds 500,000, or the person has insufficient contact information.

Substitute notice consists of:

(1) email notice when the person has an email address for the subject persons;

(2) conspicuous posting of the notice on the website page of the person, if the person maintains one; and

(3) notification to major statewide media. S.C. Code § 39-1-90(E).

WHAT MUST THE NOTICE SAY?

The statute does not specify the contents of the notification.

ARE THERE ANY EXEMPTIONS?

A person 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 the statute is considered to be in compliance with the notification requirements of the statute if the person notifies subject persons in accordance with its policies in the event of a breach of security of the system. S.C. Code § 39-1-90(F).

This statute does not apply to a bank or financial institution that is subject to and in compliance with the privacy and security provision of the Gramm-Leach-Bliley Act. S.C. Code § 39-1-90(I).

A financial institution that is subject to and in compliance with the federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice, issued March 7, 2005, by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision, as amended, is considered to be in compliance with the statute. S.C. Code § 39-1-90(J).

WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

The Department of Consumer Affairs may impose fines of up to $1,000 per affected resident for a knowing and willful violation of the statute. S.C. Code § 39-1-90(H). Private rights of action are also available. S.C. Code § 39-1-90(G).

ARE THERE ANY DATA SECURITY REQUIREMENTS IMPOSED?

No.

ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

South Carolina passed an Insurance Data Security Act directed specifically at the insurance industry. The act became effective on January 1, 2019. The Act requires insurance licensees to develop data protection programs "commensurate with the size and complexity of the licensee, the nature and scope of the licensee's activities, including its use of third-party service providers, and the sensitivity of the nonpublic information used by the licensee or in the licensee's possession, custody, or control." See 2018 South Carolina Laws Act 171 (H.4655).

A licensee's data protection program "must establish a written incident response plan designed to promptly respond to, and recover from, a cybersecurity event that compromises the confidentiality, integrity, or availability of nonpublic information in its possession, the licensee's information systems, or the continuing functionality of any aspect of the licensee's business or operations." *Id*.

If a licensee discovers a data security breach has occurred, it must notify the South Carolina Director of Insurance within 72 hours after determining that a breach has occurred and provide detailed information on the breach.

Back to TOC

SOUTH DAKOTA

STATUTE: S.B. No. 62.[100]

WHO MUST COMPLY?

"Information holders" - any person or business that conducts business in South Dakota, and that owns or licenses computerized personal or protected information of residents of South Dakota. S.B. No. 62 § 1(3).

WHAT DATA IS COVERED?

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

(1) Social security number;

(2) Driver license number or other unique identification number created or collected by a government body;

(3) Account, credit card, or debit card number, in combination with any required security code, access code, password, routing number, PIN, or any additional information that would permit access to a person's financial account;

(4) Health information as defined in 45 CFR 160.103; or

(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.

The term does not include information that is lawfully made available to the general public from federal, state, or local government records or information that has been redacted, or otherwise made unusable. S.B. No. 62 § 1(4).

WHAT CONSTITUTES A DATA BREACH?

The unauthorized acquisition of unencrypted computerized data or encrypted computerized data and the encryption key by any person that materially compromises the security, confidentiality, or integrity of personal or protected information maintained by the information holder. Does not include the good faith acquisition of personal or protected information by an employee or agent of the information holder for the purposes of the information holder if the personal or protected information is not used or subject to further unauthorized disclosure. S.B. No. 62 § 1(1).

[100] Publicly available at: **https://legiscan.com/SD/text/SB62/2018** (last visited June 11, 2019).

WHO MUST BE NOTIFIED?

An information holder shall disclose in accordance with section 4 of this Act the breach of system security to any resident of this state whose personal or protected information was, or is reasonably believed to have been, acquired by an unauthorized person.

Any information holder that experiences a breach of system security under this section shall disclose to the attorney general by mail or electronic mail any breach of system security that exceeds two hundred fifty residents of this state.

If an information holder discovers circumstances that require notification pursuant to section 2 of this Act the information holder shall also notify, without unreasonable delay, all consumer reporting agencies, as defined under 15 U.S.C. § 1681a in effect as of January 1, 2018, and any other credit bureau or agency that compiles and maintains files on consumers on a nationwide basis, of the timing, distribution, and content of the notice. S.B. No. 62 §§ 2, 6.

WHEN MUST NOTICE BE SENT?

A disclosure under this section shall be made not later than 60 days from the discovery or notification of the breach of system security, unless a longer period of time is required due to the legitimate needs of law enforcement as provided under section 3 of this Act.

A notification required under section 2 of this Act may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. If the notification is delayed, the notification shall be made not later than thirty days after the law enforcement agency determines that notification will not compromise the criminal investigation. S.B. No. 62 § 2.

IN WHAT FORM AND MANNER MUST NOTICE BE SENT?

A disclosure under section 2 of this Act may be provided by:

(1) Written notice;

(2) Electronic notice, if the electronic notice is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 in effect as of January 1, 2018, or if the information holder's primary method of communication with the resident of this state has been by electronic means; or

(3) Substitute notice, if the information holder demonstrates that the cost of providing notice would exceed $250,000, that the affected class of persons to be notified exceeds five hundred thousand persons, or that the information holder does not have sufficient contact information and the notice consists of each of the following:

(a) Email notice, if the information holder has an email address for the subject persons;

(b) Conspicuous posting of the notice on the information holder's website, if the information holder maintains a website page; and

(c) Notification to statewide media. S.B. No. 62 § 3.

WHAT MUST THE NOTICE SAY?

The statute does not specify the contents of the notification.

ARE THERE ANY EXEMPTIONS?

If an information holder maintains its own notification procedure as part of an information security policy for the treatment of personal or protected information and the policy is otherwise consistent with the timing requirements of this section, the information holder is in compliance with the notification requirements of section 4 of this Act if the information holder notifies each person in accordance with the information holder's policies in the event of a breach of system security.

Notwithstanding any other provisions in this Act, any information holder that is regulated by federal law or regulation, including the Health Insurance Portability and Accountability Act of 1996 (P.L. 104-191, as amended) ("HIPAA") or the Gramm Leach Bliley Act (15 U.S.C. § 6801 et seq., as amended) and that maintains procedures for a breach of system security pursuant to the laws, rules, regulations, guidance, or guidelines established by its primary or functional federal regulator is deemed to be in compliance with this chapter if the information holder notifies affected South Dakota residents in accordance with the provisions of the applicable federal law or regulation. S.B. No. 62 §§ 5, 8.

WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

The Attorney General may prosecute each failure to disclose under the provisions of this Act as a deceptive act or practice under § 37-24-6. In addition to any remedy provided under chapter 37-24, SB No. 62, the Attorney General may bring an 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 attorney's fees and any costs associated with any action brought under this section. S.B. No. 62 § 7.

ARE THERE ANY DATA SECURITY REQUIREMENTS IMPOSED?

No.

ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

None.

TENNESSEE

STATUTE: Tenn. Code §**47-18-2107**[101]

WHO MUST COMPLY?

A person or business that conducts business in the State, 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. Tenn. Code §§ 47–18–2107(a)(3).

WHAT DATA IS COVERED?

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

(1) social security number;

(2) driver's license number; or

(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. Tenn. Code § 47–18–2107(a)(4)(A).

Does not include information that is lawfully made available to the general public from federal, state, or local government records or information that has been redacted, or otherwise made unusable. Tenn. Code § 47–18–2107(a)(4)(B).

WHAT CONSTITUTES A DATA BREACH?

The unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the information holder. Tenn. Code § 47–18–2107(a)(1)(A).

A breach does not include the good faith acquisition of the information, as defined by the statute. Tenn. Code § 47–18–2107(a)(1)(B). In addition, the statute does not apply if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted and the unauthorized individual does not have the encryption key. Tenn. Code § 47–18–2107(a)(1)(A).

Encrypted means computerized data that is rendered unusable, unreadable, or indecipherable without the use of a decryption process or key and in accordance with the current version of the Federal Information Processing Standard (FIPS) 140-2. Tenn. Code § 47–18–2107(a)(2).

[101] Publicly available at: https://law.justia.com/codes/tennessee/2017/title-47/chapter-18/part-21/section-47-18-2107/ (last visited June 12, 2019).

WHO MUST BE NOTIFIED?

Any resident of Tennessee whose personal information has been affected. Tenn. Code § 47–18–2107(b). Any entity that maintains computerized data that includes personal information that the information holder does not own shall notify the owner or licensee of the information. Tenn. Code § 47–18–2107(c).

In addition, consumer reporting agency notification is required if more than 1,000 people are affected. Tenn. Code § 47–18–2107(g).

WHEN MUST NOTICE BE SENT?

Immediately, but no later than 45 days from the discovery or notification of the breach, unless a longer period of time is required due to the legitimate needs of law enforcement. Tenn. Code § 47–18–2107(b), (c), (d).

IN WHAT FORM AND MANNER MUST NOTICE BE SENT?

Notice must be provided by one of the following methods:

(1) written notice;

(2) electronic notice (if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001); or

(3) Substitute notice, if the information holder demonstrates that the cost of providing notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000, or the information holder does not have sufficient contact information. Tenn. Code § 47–18–2107(e).

Substitute notice consists of:

(1) email notice, when the information holder has an email address for the subject persons;

(2) conspicuous posting of the notice on the information holder's Internet website page, if the information holder maintains such website page; and

(3) notification to major statewide media. Tenn. Code § 47–18–2107(e)(3)

WHAT MUST THE NOTICE SAY?

The statute does not specify the contents of the notification.

ARE THERE ANY EXEMPTIONS?

The statute is not applicable to any person subject to Title V of the Gramm–Leach–Bliley Act of 1999 (Pub. L. No. 106–102); or the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1320D) ("HIPAA"), as expanded by the Health Information Technology for

Clinical and Economic Health Act (42 U.S.C. § 300JJ *et seq*., and 42 U.S.C. § 17921 *et seq*.) ("HITECH"). Tenn. Code § 47–18–2107(i).

WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

Private rights of action are available. Tenn. Code § 47–18–2107(h). The statute does not specify which State agency has enforcement authority, or the types of penalties, if any, may be imposed.

ARE THERE ANY DATA SECURITY REQUIREMENTS IMPOSED?

No.

ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

None.

TEXAS

STATUTE: Tex. Bus. & Com. Code §§ **521.002, 521.053**;[102] Tex. Bus. & Com. Code § **521.053**[103] **(as amended effective January 01, 2020)**; Tex. Ed. Code § **37.007(b)(5)**;[104] Tex. Pen. Code § **33.02**.[105]

WHO MUST COMPLY?

A person who conducts business in Texas and owns, licenses, or maintains computerized data that includes sensitive personal information. Tex. Bus. & Com. Code §§ 521.053(b)(c).

WHAT DATA IS COVERED?

An individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted, and the information is not publicly available:

(1) social security number;

(2) driver's license number or government issued identification number; or

(3) account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account. Tex. Bus. & Com. Code § 521.002(a)(2)(A).

In addition, information that identifies an individual and relates to:

(1) the physical or mental health or condition of the individual;

(2) the provision of health care to the individual; or

(3) payment for the provision of health care to the individual. Tex. Bus. & Com. Code § 521.002(a)(2)(B).

WHAT CONSTITUTES A DATA BREACH?

The unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt the data.

---

[102] Publicly available at: *Texas Constitution and Statutes*, www.statutes.legis.state.tx.us/Index.aspx, **http://www.statutes.legis.state.tx.us/Docs/BC/htm/BC.521.htm** (last visited June 12, 2019).
[103] Publicly available at: https://capitol.texas.gov/tlodocs/86R/billtext/pdf/HB04390F.pdf#navpanes=0 (last visited June 14, 2019).
[104] Publicly available at: *Texas Constitution and Statutes*, www.statutes.legis.state.tx.us/Index.aspx, **http://www.statutes.legis.state.tx.us/Docs/ED/htm/ED.37.htm#37.007** (last visited June 12, 2019).
[105] Publicly available at: *Texas Constitution and Statutes*, www.statutes.legis.state.tx.us/Index.aspx, http://www.statutes.legis.state.tx.us/StatutesByDate.aspx?code=PE&level=SE&value=33.02&date=7/18/2015 (last visited June 12, 2019).

Breach does not include the good faith acquisition of the information, as defined by the statute. Tex. Bus. & Com. Code § 521.053(a).

Data that is encrypted is only subject to the statute if the person accessing the data has the key required to decrypt the data. Tex. Bus. & Com. Code § 521.053(a). The statute does not define encryption.

WHO MUST BE NOTIFIED?

Any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Tex. Bus. & Com. Code § 521.053(b).

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. Tex. Bus. & Com. Code § 521.053(c).

Consumer reporting agency notification is also required if more than 10,000 people are affected. Tex. Bus. & Com. Code § 521.053(h).

WHEN MUST NOTICE BE SENT?

Disclosure shall be made without unreasonable delay and in each case not later than the 60th day after the date on which the person determines that the breach occurred. The notification shall be made as soon as the law enforcement agency determines that the notification will not compromise the investigation. Tex. Bus. & Com. Code §§ 521.053(b), (d).

A person who is required to disclose or provide notification of a breach of system security under this section shall notify the attorney general of that breach not later than the 60th day after the date on which the person determines that the breach occurred if the breach involves at least 250 residents of Texas.

The notification under this subsection must include:

(1) a detailed description of the nature and circumstances of the breach or the use of sensitive personal information acquired as a result of the breach;

(2) the number of Texas residents affected by the breach at the time of notification;

(3) the measures taken by the person regarding the breach;

(4) any measures the person intends to take regarding the breach after the notification under this subsection; and

(5) information regarding whether law enforcement is engaged in investigating the breach. Tex. Bus. & Com. Code § 521.053(b).

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. Tex. Bus. & Com. Code § 521.053(c).

IN WHAT FORM AND MANNER MUST NOTICE BE SENT?

Notice must be provided by one of the following methods:

(1) written notice to individual's last known address;

(2) electronic notice; or

(3) other notice, where the entity demonstrates that the cost of providing notice would exceed $250,000, the number of affected persons exceeds 500,000, or the person does not have sufficient contact information.

Other notice must be given by:

(1) Electronic mail, if the person has electronic mail addresses for the affected persons;

(2) conspicuous posting of the notice on the person's website; or

(3) notice published in or broadcast on major statewide media. Tex. Bus. & Com. Code §§ 521.053(e), (f).

WHAT MUST THE NOTICE SAY?

The statute does not specify the contents of the notification.

ARE THERE ANY EXEMPTIONS?

A person is deemed in compliance with the statute if it maintains and complies with its own notification procedures as part of an information security policy and whose procedures are consistent with the timing requirements of the statute. Tex. Bus. & Com. Code § 521.053(g). Good faith acquisition of sensitive personal information by an employee or agent of the covered entity for the purposes of the covered entity is not subject to notification so long as the sensitive personal information is not used or disclosed in an unauthorized manner. Tex. Bus. & Com. Code § 521.053(a).

WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

The Attorney General has enforcement authority. Violations may result in civil fines of at least $2,000 but not more than $50,000 per violation. Tex. Bus. & Com. Code § 521.151(a). Fines of $100 per individual to whom notification is due for each day that reasonable action to comply with the statute is not taken – up to $250,000. Tex. Bus. & Com. Code § 521.151(a-1). The Attorney General is entitled to recover reasonable expenses including reasonable attorney fees,

court costs, and investigatory costs incurred in obtaining injunctive relief or civil penalties. Tex. Bus. & Com. Code § 521.151(f).

ARE THERE ANY DATA SECURITY REQUIREMENTS IMPOSED?

A business shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect from unlawful use or disclosure any sensitive personal information collected or maintained by the business in the regular course of business. Tex. Bus. & Com. Code § 521.052(a).

A business shall destroy or arrange for the destruction of customer records containing sensitive personal information within the business's custody or control that are not to be retained by the business by:

(1) shredding;

(2) erasing; or

(3) otherwise modifying the sensitive personal information in the records to make the information unreadable or indecipherable through any means. Tex. Bus. & Com. Code § 521.052(b).

ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

Pursuant to H.B. No. 4390, which goes into effect on January 01, 2020, a Texas Privacy Protection Advisory Council is created to study data privacy laws in the State, other states, and relevant foreign jurisdictions. Tex. Bus. & Com. Code § 521.053§ 2(b).

The council is composed of members who are residents of Texas and appointed as follows:

(1) five members appointed by the speaker of the house of representatives, two of whom must be representatives of an industry listed under Subsection (d) of this section and three of whom must be members of the house of representatives;

(2) five members appointed by the lieutenant governor, two of whom must be representatives of an industry listed under Subsection (d) of this section and three of whom must be senators; and

(3) five members appointed by the governor, three of whom must be representatives of an industry listed under Subsection (d) of this section and two of whom must be either: (A) a representative of a nonprofit organization that studies or evaluates data privacy laws or (B) a professor who teaches at a law school in Texas or other institution of higher education, as defined by Section 61.003, Education Code. Tex. Bus. & Com. Code § 521.053§ 2(c), (d).

UTAH

STATUTE: Utah Code §§ 13-44-101 ***et seq*. (section 13-44-301 amended May 9, 2017)**,[106] **53A-13-301**.[107]

WHO MUST COMPLY?

Any person who owns, licenses or maintains computerized data that includes personal information concerning a Utah resident. Utah Code § 13-44-202(1), (3).

WHAT DATA IS COVERED?

Personal information means a person's first name or first initial and last name, combined with any one or more of the following data elements relating to that person when either the name or date element is unencrypted or not protected by another method that renders the data unreadable or unusable:

(1) social security number;

(2) financial account number, or credit or debit card number; and (B) any required security code, access code, or password that would permit access to the person's account; or

(3) driver license number or state identification card number.

Personal information does not include information regardless of its source, contained in federal, state, or local government records or in widely distributed media that are lawfully made available to the general public. Utah Code § 13-44-102(4)(a)(b).

WHAT CONSTITUTES A DATA BREACH?

Breach of system security means an unauthorized acquisition of computerized data maintained by a person that compromises the security, confidentiality, or integrity of personal information. Utah Code § 13-44-102(1)(a).

Breach of system security does not include the acquisition of personal information by an employee or agent of the person possessing unencrypted computerized data unless the personal information is used for an unlawful purpose or disclosed in an unauthorized manner. Utah Code § 13-44-102(1)(b).

[106] Publicly available at: *Utah State Legislature*, http://le.utah.gov/xcode/Title13/Chapter44/13-44.html?v=C13-44_1800010118000101 (last visited June 17, 2019).
[107] Publicly available at: *Utah State Legislature*, **https://le.utah.gov/~2018/bills/static/HB0010.html** (last visited June 17, 2019).

WHO MUST BE NOTIFIED?

Any resident of Utah whose personal information has been affected. Utah Code § 13-44-202(1)(a).

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 of system. Utah Code § 13-44-202(3)(a).

WHEN MUST NOTICE BE SENT?

Notice must be provided in the most expedient time possible without unreasonable delay taking into account:

(1) legitimate investigative needs of law enforcement;

(2) investigation of the scope of the breach of system security; and

(3) restoration of the reasonable integrity of the system. Utah Code § 13-44-202(2).

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 of system security immediately following the person's discovery of the breach if misuse of the personal information occurs or is reasonably likely to occur. Utah Code § 13-44-202(3)(a).

IN WHAT FORM AND MANNER MUST NOTICE BE SENT?

A notification required by the statute must be provided in one of the following manners:

(1) in writing by first-class mail to the most recent address the person has for the resident;

(1) electronically, if the person's primary method of communication with the resident is by electronic means, or if provided in accordance with the consumer disclosure provisions of 15 U.S.C. § 7001;

(2) by telephone, including through the use of automatic dialing technology not prohibited by other law; or

(3) by publishing notice of the breach of system security in a newspaper of general circulation and in accordance with the legal notice publication requirements of § 45-1-101. Utah Code § 13-44-202(5).

WHAT MUST THE NOTICE SAY?

The statute does not specify the contents of the notification.

ARE THERE ANY EXEMPTIONS?

Yes. If a person maintains the person's own notification procedures as part of an information security policy for the treatment of personal information the person is considered to be in compliance with this chapter's notification requirements if the procedures are otherwise consistent with this chapter's timing requirements and the person notifies each affected Utah resident in accordance with the person's information security policy in the event of a breach. Utah Code § 13-44-202(5)(b).

In addition, a person who is regulated by state or federal law and maintains procedures for a breach of system security under applicable law established by the primary state or federal regulator is considered to be in compliance with this part if the person notifies each affected Utah resident in accordance with the other applicable law in the event of a breach. Utah Code § 13-44-202(5)(c).

WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

The Attorney General may enforce this chapter's provisions. Nothing in this chapter creates a private right of action. And nothing in this chapter affects any private right of action existing under other law, including contract or tort. Utah Code § 13-44-301(2).

A person who violates this chapter's provisions is subject to a civil fine of no greater than $2,500 for a violation or series of violations concerning a specific consumer; and no greater than $100,000 in the aggregate for related violations concerning more than one consumer. Utah Code § 13-44-301(3).

In addition, the Attorney General may seek injunctive relief to prevent future violations of this chapter in the district court located in Salt Lake City; or the district court for the district in which resides a consumer who is affected by the violation. The Attorney General may also seek attorney fees and costs. Utah Code § 13-44-301(4)(a),(b).

ARE THERE ANY DATA SECURITY REQUIREMENTS IMPOSED?

Any person who conducts business in the state of Utah and maintains personal information shall implement and maintain reasonable procedures to:

(a) prevent unlawful use or disclosure of personal information collected or maintained in the regular course of business; and

(b) 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:

(a) shredding;

(b) erasing; or

(c) otherwise modifying the personal information to make the information indecipherable. Utah Code § 13-44-201.

ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

None.

VERMONT

STATUTE: Vt. Stat. Ann. tit. 9 §§ **2430**,[108] **2435**.[109]

WHO MUST COMPLY?

Any data collector that maintains or possesses computerized data containing personally identifiable information of a consumer that the data collector does not own or license, 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. Vt. Stat. Ann. tit. 9 § 2435(b)(2).

"Data collector" means a person who, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates, or otherwise deals with personally identifiable information, and includes the State, State agencies, political subdivisions of the State, public and private universities, privately and publicly held corporations, limited liability companies, financial institutions, and retail operators. Vt. Stat. Ann. tit. 9 § 2430(6).

WHAT DATA IS COVERED?

A consumer's first name or first initial and 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 or redacted or protected by another method that renders them unreadable or unusable by unauthorized persons, and the information is not publicly available:

(1) social security number;

(2) motor vehicle operator's license number or non-driver identification card number;

(3) financial account number or credit or debit card number, if circumstances exist in which the number could be used without additional identifying information, access codes, or passwords; or

(4) account passwords or personal identification numbers or other access codes for a financial account. Vt. Stat. Ann. tit. 9 § 2430(9)(A).

"Encryption" means use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without use of a confidential process or key. Vt. Stat. Ann. tit. 9 § 2430(7).

"Redaction" means the rendering of data so that the data are unreadable or are truncated so that no more than the last four digits of the identification number are accessible as part of the data. Vt. Stat. Ann. tit. 9 § 2430(11).

---

[108] Publicly available at: *Vermont General Assembly*, http://legislature.vermont.gov/, **http://legislature.vermont.gov/statutes/section/09/062/02430** (last visited June 17, 2019).
[109] Publicly available at: *Vermont General Assembly*, http://legislature.vermont.gov/, **http://legislature.vermont.gov/statutes/section/09/062/02435** (last visited June 17, 2019).

Personally identifiable information does not mean publicly available information that is lawfully made available to the general public from federal, State, or local government records. Vt. Stat. Ann. tit. 9 § 2430(9)(B).

WHAT CONSTITUTES A DATA BREACH?

The unauthorized acquisition of, electronic data or a reasonable belief of, an unauthorized acquisition of electronic data that compromises the security, confidentiality, or integrity of a consumer's personally identifiable information maintained by a data collector. Vt. Stat. Ann. tit. 9 § 2430(12)(A).

Factors to consider when determining if a breach has occurred include the following:

(1) indications that the information is in physical possession and control of unauthorized person;

(2) indications that the information has been downloaded or copied;

(3) indications that the information was used by unauthorized person; and

(4) indications that the information has been made public. Vt. Stat. Ann. tit. 9 § 2430(12)(C).

WHO MUST BE NOTIFIED?

Any resident of Vermont whose personal information has been affected. Vt. Stat. Ann. tit. 9 § 2435(b)(1).

Any data collector that maintains or possesses computerized data containing personally identifiable information of a consumer that the data collector does not own or license 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 shall notify the owner or licensee of the information of any security breach immediately following discovery of the breach. Vt. Stat. Ann. tit. 9 § 2435(b)(2).

In the event that a data collector provides notice to more than 1,000 consumers at one time, the data collector shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis. Vt. Stat. Ann. tit. 9 § 2435(c).

WHEN MUST NOTICE BE SENT?

Notice of the security breach shall be made in the most expedient time possible and without unreasonable delay, but not later than 45 days after the discovery or notification, consistent with the legitimate needs of the law enforcement agency, or with any measures necessary to determine the scope of the security breach and restore the reasonable integrity, security, and confidentiality of the data system. Vt. Stat. Ann. tit. 9 § 2435(b)(1).

Any data collector that maintains or possesses computerized data containing personally identifiable information of a consumer that the data collector does not own or license 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 shall 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. Vt. Stat. Ann. tit. 9 § 2435(b)(2).

A data collector or other entity subject to this subchapter shall provide notice of a breach to the Attorney General or to the Department of Financial Regulation, as applicable, as follows:

(1) a data collector or other entity regulated by the Department of Financial Regulation under Title 8 or this title shall provide notice of a breach to the Department. All other data collectors or other entities subject to this subchapter shall provide notice of a breach to the Attorney General; and

(2) the data collector shall notify the Attorney General or the Department, as applicable, of the date of the security breach and the date of discovery of the breach and shall provide a preliminary description of the breach within 14 business days, consistent with the legitimate needs of the law enforcement agency of the data collector's discovery of the security breach or when the data collector provides notice to consumers pursuant to the statute, whichever is sooner. Vt. Stat. Ann. tit. 9 § 2435(b)(3)(A)(B)(i).

IN WHAT FORM AND MANNER MUST NOTICE BE SENT?

A data collector must provide notice of a security breach to a consumer by one or more of the following methods:

(1) direct notice, which may be by one of the following methods:

(a) written notice mailed to the consumer's residence;

(b) electronic notice, for those consumers for whom the data collector has a valid email address if: (I) the data collector's primary method of communication with the consumer is by electronic means, the electronic notice does not request or contain a hypertext link to a request that the consumer provide personal information, and the electronic notice conspicuously warns consumers not to provide personal information in response to electronic communications regarding security breaches; or (II) the notice is consistent with the provisions regarding electronic records and signatures for notices in 15 U.S.C. § 7001; or

(c) telephonic notice, provided that telephonic contact is made directly with each affected consumer and not through a prerecorded message; or

(2) Substitute notice, if:

(a) the data collector demonstrates that the cost of providing written or telephonic notice to affected consumers would exceed $5,000.00;

(b) the class of affected consumers to be provided written or telephonic notice exceeds 5,000; or

(c) the data collector does not have sufficient contact information. Vt. Stat. Ann. tit. 9 § 2435(b)(6).

A data collector shall provide substitute notice by: (i) conspicuously posting the notice on the data collector's website if the data collector maintains one; and (ii) notifying major statewide and regional media. Vt. Stat. Ann. tit. 9 § 2435(b)(6).

WHAT MUST THE NOTICE SAY?

Notice must be clear and conspicuous and include a description of: the incident in general terms, approximate date of the breach, the type of personally identifiable information that was subject to the security breach, the general acts of the data collector to protect the personally identifiable information from further security breach, a telephone number (toll-free if available) that the consumer may call for further information and assistance, and advice that directs the consumer to remain vigilant by reviewing account statements and monitoring free credit reports. Vt. Stat. Ann. tit. 9 § 2435(b)(5).

Notice to the Attorney General or the Department will include the date, discovery, and preliminary description of the security breach and the number of Vermont individuals affected. Vt. Stat. Ann. tit. 9 § 2435(3)(B)(i), (C)(i).

ARE THERE ANY EXEMPTIONS?

Entities with their own notification policies consistent with the act may be exempt if they provide the Attorney General with information regarding the date, discovery, and description of the breach.

Notice is not required if the entity establishes that misuse of the personal identifiable information is not reasonably possible and the entity provides notice of its determination that the misuse of the information is not reasonably possible to the Attorney General or Department of Financial Regulation (as applicable). Vt. Stat. Ann. tit. 9 § 2435(d)(1).

WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

With respect to all data collectors and other entities subject to this subchapter, other than a person or entity licensed or registered with the Department of Financial Regulation under Title 8 or this title, the Attorney General and State's Attorney shall have sole and full authority to investigate potential violations of this subchapter and to enforce, prosecute, obtain, and impose remedies for a violation of this subchapter or any rules or regulations made pursuant to this chapter as the Attorney General and State's Attorney have under chapter 63 of this title. The Attorney General may refer the matter to the State's Attorney in an appropriate case. The

Superior Courts shall have jurisdiction over any enforcement matter brought by the Attorney General or a State's Attorney under this subsection. Vt. Stat. Ann. tit. 9 § 2435(g)(1).

With respect to a data collector that is a person or entity licensed or registered with the Department of Financial Regulation under Title 8 or this title, the Department of Financial Regulation shall have the full authority to investigate potential violations of this subchapter and to prosecute, obtain, and impose remedies for a violation of this subchapter or any rules or regulations adopted pursuant to this subchapter, as the Department has under Title 8 or this title or any other applicable law or regulation. Vt. Stat. Ann. tit. 9 § 2435(g)(2).

ARE THERE ANY DATA SECURITY REQUIREMENTS IMPOSED?

No.

ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

On August 6, 2013, the Vermont Department of Financial Regulation issued Bulletin Number 3, which summarizes the notice requirements in the Vermont Security Breach Notification Act, codified at Vt. Stat. Ann. tit. 9 §§ 2435(b) and (f). The Bulletin provides that Vermont's breach notification law applies to insurance companies, captive insurance companies, debt adjusters, and any other public or private corporation, limited liability company, or business regulated by the Department. The Bulletin further provides that any entity regulated by the Department must provide notice to the Department within 14 days of discovering any electronic data security breach that compromises a consumer's nonpublic personally identifiable information.

VIRGINIA

STATUTE: Va. Code §§ **18.2-186.6 (as amended Mar. 13, 2017)**,[110] **32.1-127.1:05**,[111] **22.1-20.2**.[112]

WHO MUST COMPLY?

Individuals and entities that own, license, or maintain computerized data that includes personal information regarding Virginia residents. Va. Code § 18.2-186.6(B), (D).

WHAT DATA IS COVERED?

The first name or first initial and last name in combination with, and linked to, any one or more of the following data elements that relate to a Virginia resident, when the data elements are neither encrypted nor redacted:

(1) social security number;

(2) driver's license number or state identification card number issued in lieu of a driver's license number; or

(3) financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial accounts.

Personal Information does not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public. Va. Code § 18.2-186.6(A).

WHAT CONSTITUTES A DATA BREACH?

The unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes, or the individual or entity reasonably believes has caused, or will cause, identity theft or other fraud to any resident of Virginia. Va. Code § 18.2-186.6(A).

Breach does not include the good faith acquisition of the information, as defined by the statute. Nor does the statute apply to data that is encrypted or redacted. The statute applies if data is encrypted but the encryption is compromised as a result of the breach. Va. Code § 18.2-186.6(A), (C).

---

[110] Publicly available at: *Virginia Law*, https://law.lis.virginia.gov/vacode/title18.2/chapter6/section18.2-186.6/ (last visited June 17, 2019).
[111] Publicly available at: *Virginia Law*, https://law.lis.virginia.gov/vacode/title32.1/chapter5/section32.1-127.1 (last visited June 17, 2019).
[112] Publicly available at: *Virginia Law*, https://law.lis.virginia.gov/vacode/title22.1/chapter2/section22.1-20.2/ (last visited June 17, 2019).

"Encrypted" means that transformation of data through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without the use of a confidential process or key, or the securing of the information by another method that renders the data elements unreadable or unusable. Va. Code § 18.2-186.6(A).

"Redact" means alteration or truncation of data such that no more than the following are accessible as part of the personal information: (1) five digits of a social security number; or (2) the last four digits of a driver's license number, state identification card number, or account number. Va. Code § 18.2-186.6(A).

WHO MUST BE NOTIFIED?

The Attorney General, and any affected resident of Virginia. Va. Code § 18.2-186.6(B).

In the event that an individual or entity provides notice to more than 1,000 persons at one time, the individual or entity shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. § 1681a(p), of the timing, distribution, and content of the notice. Va. Code § 18.2-186.6(E).

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. Va. Code § 18.2-186.6(D).

WHEN MUST NOTICE BE SENT?

Notice must be sent without unreasonable delay upon discovery of the breach. Notice required by the statute may be reasonably delayed to allow the individual or entity to determine the scope of the breach of the security of the system and restore the reasonable integrity of the system. Va. Code § 18.2-186.6(B).

Notice required by the statute may be delayed if, after the individual or entity notifies a law enforcement agency, the 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. Va. Code § 18.2-186.6(B).

Notice shall be made without unreasonable delay after the law enforcement agency determines that the notification will no longer impede the investigation or jeopardize national or homeland security. Va. Code § 18.2-186.6(B).

IN WHAT FORM AND MANNER MUST NOTICE BE SENT?

Notice must be provided by one of the following methods:

(1) written notice to individual's last known address;

(2) telephone notice;

(3) electronic notice; or

(4) Substitute notice, if the individual or the entity required to provide notice demonstrates that the cost of providing notice will exceed $50,000, the affected class of Virginia residents to be notified exceeds 100,000 residents, or the individual or the entity does not have sufficient contact information or consent to provide notice as described in subdivisions .

Substitute notice must be provided as follows:

(1) email notice, if the individual or the entity has email addresses for the members of the affected class of residents;

(2) conspicuous posting of the notice on the website of the individual or the entity, if the individual or the entity maintains a website; and

(3) notice to major statewide media. Va. Code § 18.2-186.6(A)(4).

WHAT MUST THE NOTICE SAY?

Notice shall include a description of the incident in general terms, the type of personal information that was subject to the unauthorized access and acquisition, the general acts of the individual or entity to protect the personal information from further unauthorized access, a telephone number that the person may call for further information and assistance, if one exists, and advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports. Va. Code § 18.2-186.6(A)(4).

In the instance of a breach of tax information the Office of the Attorney General must be notified with the name and federal employer identification number of the employer as defined in § 58.1–460 that may be affected by the compromise in confidentiality. Va. Code § 18.2-186.6(M).

ARE THERE ANY EXEMPTIONS?

The provisions of the statute shall not apply to criminal intelligence systems subject to the restrictions of 28 C.F.R. Part 23 that are maintained by law-enforcement agencies of the Commonwealth and the Organized Criminal Gang File of the Virginia Criminal Information Network ("VCIN"). Va. Code § 18.2-186.6(L).

An entity that complies with the notification requirements or procedures pursuant to the rules, regulations, procedures, or guidelines established by the entity's primary or functional state or federal regulator shall be in compliance with the statute. Va. Code § 18.2-186.6(H).

WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

Virginia allows enforcement by the Attorney General, or the entity's primary state Corporation Commission. Va. Code § 18.2-186.6(K). Violations prosecuted by the Virginia Attorney General can result in penalties up to $150,000 per breach. Va. Code § 18.2-186.6(I).

Virginia also allows a private right of action. Va. Code § 18.2-186.6(I).

ARE THERE ANY DATA SECURITY REQUIREMENTS IMPOSED?

No.

ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

A violation of the statute by a state-chartered or licensed financial institution shall be enforceable exclusively by the financial institution's primary state regulator. Va. Code § 18.2-186.6(J).

The Department of Education shall develop, in collaboration with the Virginia Information Technologies Agency, and update regularly but in no case less than annually, a model data security plan for the protection of student data held by school divisions. The Department of Education shall designate a Chief Data Security Officer, with such State funds as made available, to assist school divisions, upon request, with the development and implementation of their own data security plans and to develop best practice recommendations regarding the use, retention, and protection of student data. Va. Code Ann. § 22.1-20.2.

Any employer or payroll service provider that owns or licenses computerized data relating to income tax withheld pursuant to Article 16 (§§ 58.1–460, *et seq.*) of Chapter 3 of Title 58.1 shall notify the Office of the Attorney General without unreasonable delay after the discovery or notification a breach that includes taxpayer identification number in combination with the income tax withheld for that taxpayer that compromises the confidentiality of such data and that creates a reasonable belief that an unencrypted and unredacted version of such information was accessed and acquired by an unauthorized person, and causes, or the employer or payroll provider reasonably believes has caused or will cause, identity theft or other fraud. Va. Code § 18.2-186.6(M).

VIRGIN ISLANDS

STATUTE: V.I. Code 14 § **2208, *et seq*.**[113]

WHO MUST COMPLY?

Any agency that owns, maintains or licenses computerized data that includes personal information. V.I. Code 14 § 2208 (a), (b).

WHAT DATA IS COVERED?

"Personal information," meaning an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(1) social security number;

(2) driver's license number; or

(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. V.I. Code 14 § 2208(e).

"Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or territorial government records. V.I. Code 14 § 2208(f).

The statute does not apply if the affected data is encrypted. V.I. Code 14 § 2208(a), (e).

WHAT CONSTITUTES A DATA BREACH?

The unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure. V.I. Code 14 § 2208(d).

WHO MUST BE NOTIFIED?

Any resident of the Virgin Islands whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. V.I. Code 14 § 2208(a).

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. V.I. Code 14 § 2208(b).

---

[113] Publicly available at: **https://www.dwt.com/files/Uploads/Documents/Publications/VirginIslands%20Security%20Breach.pdf**.

WHEN MUST NOTICE BE SENT?

Notification must be sent immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. V.I. Code 14 § 2208(a).

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. V.I. Code 14 § 2208(b).

The notification required by the statute may be delayed, if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by the statute must be made after the law enforcement agency determines that it will not compromise the investigation. V.I. Code 14 § 2208(a).

IN WHAT FORM AND MANNER MUST NOTICE BE SENT?

"Notice" must be provided by one of the following methods:

(1) written notice;

(2) electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures; or

(3) Substitute notice, if the agency demonstrates that the cost of providing notice would exceed $100,000, or that the affected class of subject persons to be notified exceeds 50,000, or the agency does not have sufficient contact information.

Substitute notice shall consist of all of the following:

(1) email notice when the agency has an email address for the subject persons;

(2) conspicuous posting of the notice on the agency's Web site page, if the agency maintains one; and

(3) notification to major territory-wide media. V.I. Code 14 § 2208(g).

WHAT MUST THE NOTICE SAY?

The statute does not specify the contents of the notification.

ARE THERE ANY EXEMPTIONS?

An agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of the statute shall be deemed to be in compliance with the notification

requirements of the statute if it notifies subject persons in accordance with its policies in the event of a breach of security of the system. V.I. Code 14 § 2208(h).

WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

Not specified.

ARE THERE ANY DATA SECURITY REQUIREMENTS IMPOSED?

No.

ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

None.

WASHINGTON

STATUTE: Wash. Rev. Code §§ **19.255.010**,[114] **42.56.590**.[115]

WHO MUST COMPLY?

Any person or business that conducts business in the State and that owns, licenses or maintains data that includes personal information. Wash. Rev. Code §§ 19.255.010(1), (2).

Any agency that owns or licenses data that includes personal information. Wash. Rev. Code § 42.56.590(1)(a).

WHAT DATA IS COVERED?

"Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements:

(1) social security number;

(2) driver's license number or Washington identification card number; or

(3) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. Wash. Rev. Code § 19.255.010(5).

The breach of secured personal information must be disclosed if the information acquired and accessed is not secured during a security breach or if the confidential process, encryption key, or other means to decipher the secured information was acquired by an unauthorized person. Wash. Rev. Code § 19.255.010(1).

"Secured" means encrypted in a manner that meets or exceeds the National Institute of Standards and Technology ("NIST") standard or is otherwise modified so that the personal information is rendered unreadable, unusable, or undecipherable by an unauthorized person. Wash. Rev. Code § 19.255.010(7).

"Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. Wash. Rev. Code § 19.255.010(6).

WHAT CONSTITUTES A DATA BREACH?

The unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach

[114] Publicly available at: *Washington State Legislature*, http://leg.wa.gov/, http://apps.leg.wa.gov/RCW/default.aspx?cite=19.255.010 (last visited June 24, 2019).
[115] Publicly available at: *Washington State Legislature*, http://leg.wa.gov/, http://apps.leg.wa.gov/RCW/default.aspx?cite=42.56.590 (last visited June 24, 2019).

of the security of the system when the personal information is not used or subject to further unauthorized disclosure. Wash. Rev. Code § 19.255.010(4).

Notice is not required if the breach of the security of the system is not reasonably likely to subject consumers to a risk of harm. Wash. Rev. Code § 19.255.010(1).

WHO MUST BE NOTIFIED?

Any resident of the State whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the personal information was not secured. Wash. Rev. Code § 19.255.010(1).

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. Wash. Rev. Code § 19.255.010(2).

Any person or business that is required to issue a notification pursuant to the statute to more than 500 Washington residents as a result of a single breach shall, by the time notice is provided to affected consumers, electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. The person or business shall also provide to the Attorney General the number of Washington consumers affected by the breach, or an estimate if the exact number is not known. Wash. Rev. Code § 19.255.010(15).

WHEN MUST NOTICE BE SENT?

Notification to affected individuals and to the Attorney General must be made in the most expedient time possible and without unreasonable delay, no more than 45 calendar days after the breach was discovered, unless at the request of law enforcement, or due to any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. Wash. Rev. Code § 19.255.010(16).

IN WHAT FORM AND MANNER MUST NOTICE BE SENT?

Notice must be provided by one of the following methods:

(1) written notice;

(2) electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures; or

(3) substitute notice, if the agency demonstrates that the cost of providing notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000, or the agency does not have sufficient contact information.

Substitute notice shall consist of all of the following:

(1) email notice when the agency has an email address for the subject persons;

(2) conspicuous posting of the notice on the agency's web site page, if the agency maintains one; and

(3) notification to major statewide media. Wash. Rev. Code § 19.255.010(8).

WHAT MUST THE NOTICE SAY?

The notification must be written in plain language and must include, at a minimum, the following information:

(1) the name and contact information of the reporting agency subject to the statute;

(2) a list of the types of personal information that were, or are reasonably believed to have been, the subject of a breach; and

(3) the toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed personal information. Wash. Rev. Code § 19.255.010(14).

ARE THERE ANY EXEMPTIONS?

A covered entity under the federal Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1320d *et seq*.) ("HIPAA") is deemed to have complied with the requirements of the statute with respect to protected health information if it has complied with § 13402 of the federal Health Information Technology for Economic and Clinical Health Act, Public Law 111-5 ("HITECH"). Wash. Rev. Code § 19.255.010(10).

WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

The Attorney General may bring an action in the name of the State, or as *parens patriae* on behalf of persons residing in the State, to enforce the statute. Wash. Rev. Code § 19.255.010(17).

The Attorney General may *not* seek treble damages under Washington's Unfair Business Practices law for a violation of the statute. Wash. Stat. § 19.86.090. Wash. Rev. Code § 19.255.010(17).

ARE THERE ANY DATA SECURITY REQUIREMENTS IMPOSED?

If a business fails to take reasonable care to guard against unauthorized access to account information that is in the possession or under the control of the business, and the failure is found to be the proximate cause of a breach, the processor or business is liable to a financial institution for reimbursement of reasonable actual costs related to the reissuance of credit cards and debit cards that are incurred by the financial institution to mitigate potential current or future damages to its credit card and debit card holders that reside in the state of Washington as a consequence of the breach, even if the financial institution has not suffered a physical injury in connection with the breach. In any legal action brought pursuant to this subsection, the prevailing party is entitled

to recover its reasonable attorneys' fees and costs incurred in connection with the legal action. Wash. Rev. Code § 19.255.020(3)(a).

ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

Yes. All licensees, including insurers and producers, are required to notify the Washington Insurance Commissioner about the number of customers or consumers potentially affected and what actions are being taken in writing within 2 business days after determining notification must be sent to consumers or customers.

The written notification should be provided to Mary Childers, Consumer Advocacy Program Manager, Washington State Office of the Insurance Commissioner, Insurance 5000 Building, P.O. Box 40256, Olympia, WA 98504-0256; e-mail: marych@oic.wa.gov.

WEST VIRGINIA

STATUTE: W.Va. Code § **46A-2A-101** ***et seq.***[116]

WHO MUST COMPLY?

Individuals or entities that own, license, or maintain computerized data that includes personal information regarding a resident of West Virginia. W.Va. Code §§ 46A-2A-102(a), (c).

WHAT DATA IS COVERED?

The first name or first initial and last name linked to any one or more of the following data elements that relate to a resident of West Virginia, when the data elements are neither encrypted nor redacted:

(1) social security number;

(2) driver's license number or state identification card number issued in lieu of a driver's license; or

(3) financial account number, or credit card, or debit card number in combination with any required security code, access code or password that would permit access to a resident's financial accounts. W.Va. Code § 46A-2A-101(6).

Personal Information does not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public. W.Va. Code § 46A-2A-101(6).

"Encrypted" means transformation of data through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key, or securing the information by another method that renders the data elements unreadable or unusable. W.Va. Code § 46A-2A-101(3).

WHAT CONSTITUTES A DATA BREACH?

The unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes the individual or entity to reasonably believe that the breach of security has caused or will cause identity theft or other fraud to any resident of West Virginia. W.Va. Code § 46A-2A-101(1).

Breach does not include the good faith acquisition of the information, as defined by the statute. W.Va. Code § 46A-2A-101(1).

[116] Publicly available at: https://codes.findlaw.com/wv/chapter-46a-west-virginia-consumer-credit-and-protection-act/wv-code-sect-46a-2a-101.html, (last visited June 25, 2019).

WHO MUST BE NOTIFIED?

Any resident of West Virginia if the entity knows that the breach has caused, or reasonably believes that the breach will cause, identity theft or other fraud of the resident. W.Va. Code § 46A-2A-102(a).

Consumer reporting agencies must be notified by the entity in cases where the notice must be provided to over 1,000 people. W.Va. Code § 46A-2A-102(f).

An individual or entity that maintains covered data must notify the owner or licensee of that data. W.Va. Code § 46A-2A-102(c).

WHEN MUST NOTICE BE SENT?

Except as provided in the law enforcement exception or in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the system, the notice shall be made without unreasonable delay. Notice required by this section may be delayed if a law enforcement agency determines and advises the individual or entity that the notice will impede a criminal investigation.

An individual or entity that maintains covered data must notify the owner or licensee of that data as soon as practicable following discovery. W.Va. Code § 46A-2A-102(c).

IN WHAT FORM AND MANNER MUST NOTICE BE SENT?

Notice must be provided by one of the following methods:

(1) written notice;

(2) telephonic notice;

(3) electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures; or

(4) Substitute notice, if the individual or the entity required to provide notice demonstrates that the cost of providing notice will exceed $50,000, or that the affected class of residents to be notified exceeds 100,000 persons, or that the individual or the entity does not have sufficient contact information or to provide notice as described in (1)-(3). W.Va. Code § 46A-2A-101(7).

Substitute notice consists of any two of the following:

(1) email notice if the individual or the entity has email addresses for the members of the affected class of residents;

(2) conspicuous posting of the notice on the website of the individual or the entity if the individual or the entity maintains a website; or

(3) notice to major statewide media. W.Va. Code § 46A-2A-101(7)(D).

WHAT MUST THE NOTICE SAY?

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; and

(b) whether or not the entity maintained information about that individual; and

(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. W.Va. Code § 46A-2A-102(d).

ARE THERE ANY EXEMPTIONS?

Yes. An entity that maintains its own notification procedures as part of an information privacy or security policy for the treatment of personal information and that are consistent with the timing requirements of the statute shall be deemed to be in compliance with the notification requirements of the statute if it notifies residents of the State in accordance with its procedures in the event of a breach of security of the system. W.Va. Code § 46A-2A-103(a).

In addition, a financial institution that responds in accordance with the notification guidelines prescribed by the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice is deemed to be in compliance with the statute. W.Va. Code § 46A-2A-103(b).

Further, an entity that complies with the notification requirements or procedures pursuant to the rules, regulation, procedures or guidelines established by the entity's primary or functional regulator shall be in compliance with the statute. W.Va. Code § 46A-2A-103(c).

WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

The Attorney General may enforce. Willful and repeated violations may result in penalties up to $150,000. W.Va. Code § 46A-2A-104(a)(b).

Violations by licensed financial institutions are enforced by their primary regulator. W.Va. Code § 46A-2A-104(c).

Back to TOC

ARE THERE ANY DATA SECURITY REQUIREMENTS?

No.

ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

None.

Back to TOC

WISCONSIN

STATUTE: Wis. Stat. § **134.98**.[117]

WHO MUST COMPLY?

Any entity (a person other than an individual), which does any of the following:

(1) conducts business in the State and maintains personal information in the ordinary course of business;

(2) licenses personal information in the State;

(3) maintains for a resident of the State a depository account; or

(4) lends money to a resident of the State. Wis. Stat. § 134.98(1)(a)(1).

"Entity" includes all of the following:

(1) the State and any office, department, independent agency, authority, institution, association, society, or other body in State government created or authorized to be created by the constitution or any law, including the legislature and the courts; and

(2) a city, village, town, or county. Wis. Stat. § 134.98(1)(a)(2).

WHAT DATA IS COVERED?

An individual's last name and first name or first initial, in combination with and linked to any of the following elements, if the element is not publicly available information, encrypted, redacted, or altered in a manner that renders the element unreadable:

(1) social security number;

(2) driver's license number or state identification number;

(3) financial account number, including a credit or debit card account number, or any security code, access code, or password that would permit access to the individual's financial account;

(4) DNA profile; or

(5) the individual's unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation. Wis. Stat. § 134.98(1)(b).

[117] Publicly available at: *Wisconsin State Legislature*, https://legis.wisconsin.gov/, http://docs.legis.wisconsin.gov/statutes/statutes/134/98 (last visited June 25, 2019).

"Publicly available information" is not covered and means any information that an entity reasonably believes is one of the following:

(1) lawfully made widely available through any media; or

(2) lawfully made available to the general public from federal, state, or local government records or disclosures to the general public that are required to be made by federal, state, or local law. Wis. Stat. § 134.98(1)(c).

WHAT CONSTITUTES A DATA BREACH?

Personal information acquired by an unauthorized person, or if a person, other than an individual, that stores personal information pertaining to a resident of Wisconsin, 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 that owns or licenses the personal information. Wis. Stat. § 134.98(2).

WHO MUST BE NOTIFIED?

Each resident of the State who is the subject of the personal information affected. Wis. Stat. § 134.98(2).

If an entity whose principal place of business is located in the State, or an entity that maintains or licenses personal information in the State, knows that personal information in the entity's possession has been acquired by a person whom the entity has not authorized to acquire the personal information, 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. Wis. Stat. § 134.98(2)(a).

The covered entity must notify consumer reporting agencies when notice must be provided to over 1,000 people. Wis. Stat. § 134.98(2).

WHEN MUST NOTICE BE SENT?

Notice must be sent within a reasonable time, not to exceed 45 days after learning of the breach. Reasonableness is determined based on the number of notices that must be provided and the means by which the notices will be communicated. Law enforcement may delay notification to the victims of the breach to protect an investigation or homeland security. The notification process may begin at the end of the time period set forth by law enforcement. Wis. Stat. § 134.98(3).

IN WHAT FORM AND MANNER MUST NOTICE BE SENT?

The covered entity must make reasonable efforts to notify the victim (or the person that owns or licenses the personal information) that there was a breach of data containing their 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. Wis. Stat. § 134.98(2).

Notice must be provided by mail or any other means previously used to communicate with the person. If after reasonable diligence the mailing address of the person cannot be found, and the entity has not previously communicated with the person subject to the data breach, the entity must provide notice in a method reasonably calculated to provide actual notice to the person. Wis. Stat. § 134.98(3).

Notification is not required if:

(1) the breach does not create a material risk of identity theft or fraud to the subject of the personal information; or

(2) the information was acquired in good faith by an employee or agent of the entity and for a lawful purpose. Wis. Stat. § 134.98(2)(cm).

WHAT MUST THE NOTICE SAY?

Notice shall indicate that the entity knows of the unauthorized acquisition of personal information pertaining to the subject of the personal information. Wis. Stat. §134.98(2)(a).

ARE THERE ANY EXEMPTIONS?

Yes. An entity that is subject to, and in compliance with, the privacy and security requirements of 15 U.S.C. §§ 6801 to 6827 (Protection of Nonpublic Personal Information), or a person that has a contractual obligation to such an entity, if the entity or person has in effect a policy concerning breaches of information security, is exempt. Wis. Stat. § 134.98(3m).

WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

Private rights of action are available. Other penalties are not specified in the statute.

Failure to comply with this section is not negligence or a breach of any duty, but may be evidence of negligence or a breach of a legal duty. Wis. Stat. § 134.98(4).

ARE THERE ANY DATA SECURITY REQUIREMENTS?

A financial institution, medical business or tax preparation business may not dispose of a record containing personal information unless the financial institution, medical business, tax preparation business or other person under contract with the financial institution, medical business or tax preparation business does any of the following:

(1) Shreds the record before the disposal of the record.

(2) Erases the personal information contained in the record before the disposal of the record.

(3) Modifies the record to make the personal information unreadable before the disposal of the record.

(4) Takes actions that it reasonably believes will ensure that no unauthorized person will have access to the personal information contained in the record for the period between the record's disposal and the record's destruction. Wis. Stat. § 134.97.

ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

All Wisconsin-licensed insurers, gift annuities, warranty plans, motor clubs and employee benefit plan administrators must notify the Office of the Commissioner of Insurance of any unauthorized access to personal information of Wisconsin residents as soon as practicable, but no later than 10 days after it has become aware of such unauthorized access. Wisconsin Office of the Commissioner of Insurance Bulletin (Dec. 4, 2006).

WYOMING

STATUTE: Wyo. Stat. § **40-12-501** ***et seq.***[118]

WHO MUST COMPLY?

An individual or commercial entity that conducts business in Wyoming and that owns or licenses computerized data that includes personal identifying information about a resident of Wyoming. Wyo. Stat. § 40-12-502(a). Also, any entity that maintains computerized data that includes personal identifying information on behalf of another business entity. Wyo. Stat. § 40-12-502(g).

WHAT DATA IS COVERED?

The first name or first initial and last name or any of the following data elements of an individual person:

(1) address;

(2) telephone number;

(3) social security number;

(4) driver's license number;

(5) account number, credit card number or debit card number in combination with any security code, access code or password that would allow access to a financial account of the person;

(6) tribal identification card;

(7) federal or state government issued identification card;

(8) shared secrets or security tokens that are known to be used for data based authentication;

(9) a username or email address, in combination with a password or security question and answer that would permit access to an online account;

(10) a birth or marriage certificate;

(11) medical information;

(12) health insurance information;

(13) unique biometric data; or

[118] Publicly available at: **https://codes.findlaw.com/wy/title-40-trade-and-commerce/wy-st-sect-40-12-501.html** (last visited June 25, 2019).

(14) tax identification number. Stat. § 40-12-501(a)(vii), 6-3-901(b).

Data elements that are redacted are not subject to the statute. Wyo. Stat. § 40-12-501(a)(vii). "Redact" means the alteration or truncation of data such that no more than 5 digits of the data elements set forth above are accessible. Wyo. Stat. § 40-12-501(a)(viii).

WHAT CONSTITUTES A DATA BREACH?

The unauthorized acquisition of data that materially compromises the security, confidentiality or integrity of personal identifying information maintained by a person or business and causes or is reasonably believed to cause loss or injury to a resident of Wyoming. Wyo. Stat. § 40-12-501(a)(i).

Breach does not include the good faith acquisition of the information, as defined by the statute. Wyo. Stat. § 40-12-501(a)(i).

WHO MUST BE NOTIFIED?

The resident of Wyoming whose personal identifying information was affected by the breach. Wyo. Stat. § 40-12-502(a). If the initial breach affects data maintained or held by a third-party vendor or recipient on behalf of a covered entity, that recipient must notify the covered entity. Wyo. Stat. § 40-12-502(g).

WHEN MUST NOTICE BE SENT?

The entity shall give notice as soon as possible to the affected Wyoming resident. Notice shall 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. Wyo. Stat. § 40-12-502(a).

The notification required by the statute may be delayed if a law enforcement agency determines in writing that the notification may seriously impede a criminal investigation. Wyo. Stat. § 40-12-502(b).

If the notice is sent from a third-party vendor to the owner or licensor of personal identifying information effected by a breach, it must be sent as soon as practicable following the determination that personal identifying information was, or is reasonably believed to have been, acquired by an unauthorized person. Wyo. Stat. § 40-12-502(g).

IN WHAT FORM AND MANNER MUST NOTICE BE SENT?

Notices to consumers must be provided by one of the following methods:

(1) written notice;

(2) electronic mail notice; or

(3) substitute notice. Wyo. Stat. § 40-12-502(d).

Substitute notice is an option where:

(1) the cost of providing Wyoming-based persons or businesses would exceed $10,000, and providing notice to other businesses operating but not based in the State would exceed $250,000;

(2) the number of Wyoming-based businesses or individuals would exceed 10,000, and the number of businesses operating in Wyoming to be notified would exceed 500,000; or

(3) the person does not have sufficient contact information. Wyo. Stat. § 40-12-502(d)(iii).

Substitute notice consists of:

(1) conspicuous posting on the Internet or website of the person experiencing the breach, including a toll-free number to contact the person with the data breach and the numbers for the major credit reporting agencies; and

(2) notification to major statewide media including a toll-free number where an individual can find out whether he/she is affected. Wyo. Stat. § 40-12-502(d)(iv).

The statute does not describe how a third-party vendor should send notice of a breach to owners or licensors of personal identifying information.

WHAT MUST THE NOTICE SAY?

The notification must include a description of the type of information involved in the breach, a general description of the circumstances of the breach incident, the approximate date of the breach (if reasonably possible to determine), the actions taken to protect the system from further breaches, advice directing the person to remain vigilant by reviewing account statements and monitoring credit reports, and toll-free numbers that the individual may use to contact the person collecting the data, or his agent and can learn the contact numbers for the major credit reporting agencies. Wyo. Stat. § 40-12-502(e).

ARE THERE ANY EXEMPTIONS?

A covered entity or business associate that is subject to and complies with the Health Insurance Portability and Accountability Act ("HIPAA"), and the regulations promulgated under HIPAA, 45 C.F.R. Parts 160 and 164, is deemed to be in compliance with the statute if the covered entity or business associate notifies affected Wyoming customers or entities in compliance with the requirements of HIPAA and its regulations. Wyo. Stat. § 40-12-502(h).

Back to TOC

WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

The Attorney General may bring an action in law or equity to address any violation of the statute and for other relief that may be appropriate to ensure proper compliance with the statute, to recover damages, or both. Wyo. Stat. § 40-12-502(f). No other penalty is specified in the statute.

ARE THERE ANY DATA SECURITY REQUIREMENTS?

No.

ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

None.