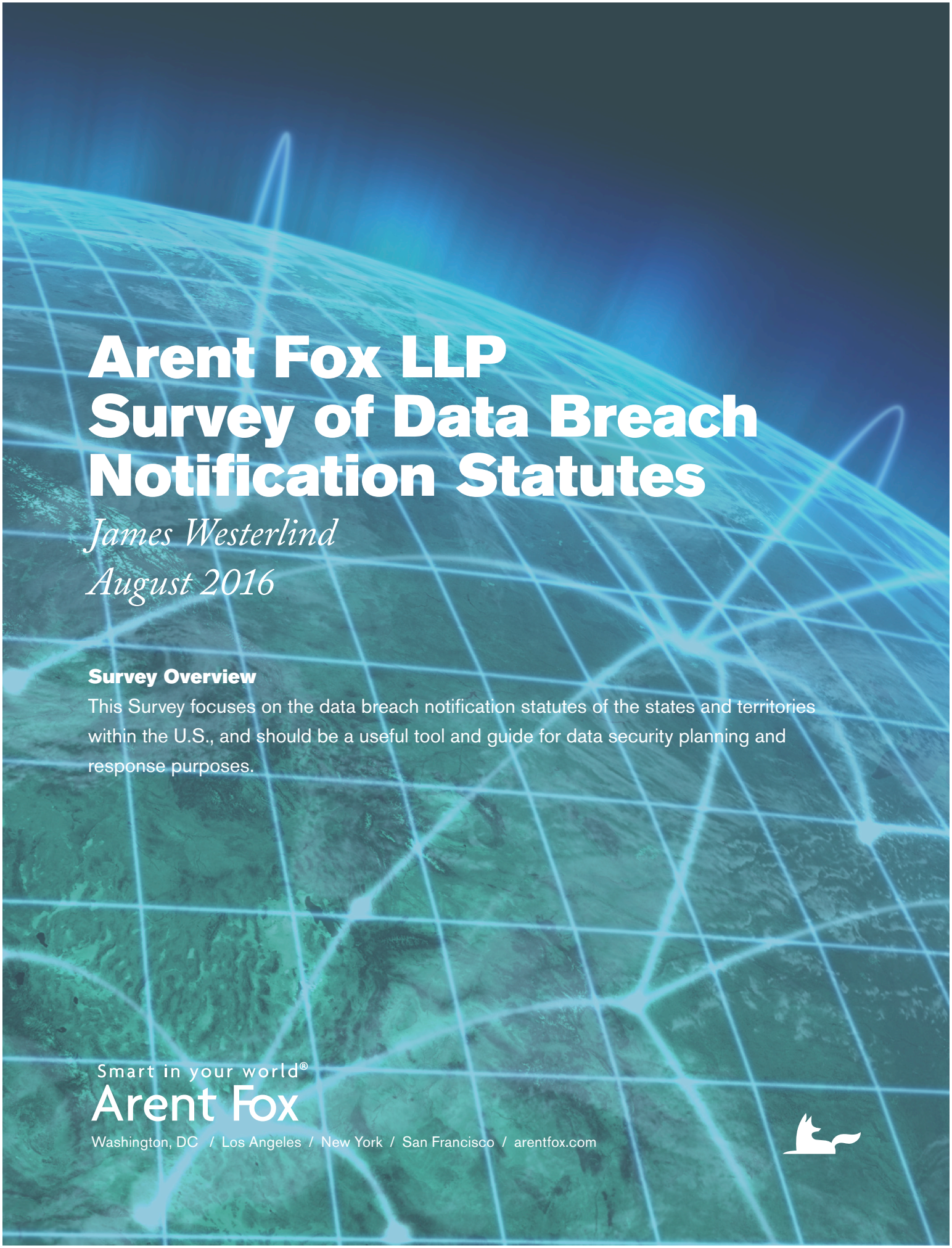

# Arent Fox LLP Survey of Data Breach Notification Statutes

*James Westerlind*

*August 2016*

**Survey Overview**

This 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.

Smart in your world®
Arent Fox
Washington, DC / Los Angeles / New York / San Francisco / arentfox.com

August 2016

We are pleased to share with you the Arent Fox LLP Survey of Data Breach Notification statutes within the United States and its territories. This Survey 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) Are there any exemptions?

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

(10) Are there any industry-specific requirements?

This 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 identifiable information may be implicated. If you have customers whose personal identifiable information may have been breached who reside in multiple jurisdictions in the U.S., 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 the company. This Survey is intended to make this 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 will supersede the Data Protection Directive and be enforceable on May 25, 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 book useful.

James Westerlind

# About the Author

## James M. Westerlind

*Counsel*, NY
212.457.5462
james.westerlind@arentfox.com

James Westerlind focuses on cyber risk issues, including insurance coverage and potential data breach liability for companies and their board members. James has also taken the lead in a number of appeals in the New York State Supreme Court, First and Second Judicial Departments, and the Second and Eleventh Circuits of the US Courts of Appeals.

## Client Work

**Insurance & Reinsurance**
James' practice also focuses on resolving insurance and reinsurance disputes, including insurance and reinsurance coverage issues on behalf of policyholders and carriers. James has also represented brokers, agents, and MGAs in disputes with insurance and reinsurance carriers.

**Litigation**
James has substantial litigation experience in both state and federal trial courts within and outside of New York, representing plaintiffs and defendants in insurance and noninsurance disputes. In addition to insurance litigation, he has defended a number of prominent US companies in product liability actions. He has also defended toxic tort cases. He has first-chaired applications for emergency relief, evidentiary hearings for emergent relief, and contempt hearings. He tried a major jury trial in the Southern District of Florida, obtaining a jury verdict finding that a life insurance policy was valid and enforceable, despite the jury finding that the trust that owned the policy made material misrepresentations in the policy's application and engaged in a civil conspiracy to defraud the insurance company and engage in a stranger-originated life insurance (STOLI) scheme. He has also defended a number of well-known tire manufacturers and large domestic retailers in product liability actions commenced in New York state and federal courts by alleged injured product users.

**Pro Bono**
James has devoted a substantial portion of his time to pro bono matters, including not-for-profit public interest endeavors and family court litigation. In fact, James is a recipient of the Arent Fox Albert E. Arent Award for outstanding pro bono achievement (Fall 2013) and the Commitment to Justice Award (February 2014) from Her Justice, a nonprofit organization devoted to helping women in need. In addition, he is a member of the Insurance Law Committee of the New York City Bar Association, where he assists in shaping New York insurance law and public policy in an effort to help the public and the profession.

## Previous Work

Prior to joining Arent Fox, James was an associate in the New York office of a large law firm.

## TABLE OF CONTENTS

**Page**

**TABLE OF CONTENTS**

**Page**

# INTRODUCTION

**By James Westerlind[1]**

Every state and territory in the U.S., except Alabama, New Mexico and South Dakota, have data breach notification statutes, and most of them 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.

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 the personal information 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. 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. 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.

Generally, notice must be provided in one of the following ways: (1) in writing; (2)

---

[1] James Westerlind is Counsel in Arent Fox's litigation, insurance, cybersecurity & data protection, and automotive practice groups. Thanks and acknowledgment to Jeff Leung, Andrew Dykens, Cesar Francia, Katarina Varriale, Carlos Estevez and Kenneth Carbajal for their hard work and assistance in the creation of this Survey.

electronically, if the entity's primary method of communication with the individual is by electronic means;[2] (3) by telephone;[3] 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(4)(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 industry-specific breach notification requirements which apply to entities handling medical records (California and Louisiana), that perform insurance functions (Georgia, Kansas, Maine and Montana), that are financial institutions (Minnesota), or are public utilities (Michigan).

[2] Some jurisdictions also allow electronic notice 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). *See, e.g.*, Alaska Stat. § 45.48.030.
[3] Missouri requires that direct contact be made with the affected individual if notice is provided by telephone. *See* Mo. Rev. Stat. § 407.1500(2).

## ALABAMA

**STATUTE:** None. Pending legislation: **H.B. 267**,[4] **H.B. 291**,[5] **S.B. 238**.[6]

H.B. 267 *Status: Pending*. Relates to public prekindergarten, elementary, and secondary education; limits the collection and disclosure of student and teacher information to specific academic purposes; provides for notification of breaches; provides civil penalties for violations.

H.B. 291 *Status: Pending*. Relates to consumer protection; requires specified entities to take generally acceptable industry practices and measures to protect and secure data containing sensitive personally identifying information in paper or electronic form; requires the entities to notify the Attorney General of data security breaches; requires notice to individuals and credit reporting agencies of data security breaches in certain circumstances; provides for the disposal of customer records.

S.B. 238 *Status: Pending*. Relates to consumer protection; requires specified entities to take generally acceptable industry practices and measures to protect and secure data containing sensitive personally identifying information in paper or electronic form; requires the entities to notify the Attorney General of data security breaches; requires notice to individuals and credit reporting agencies of data security breaches in certain circumstances; provides for the disposal of customer records.

[4] *Available at*: **http://alisondb.legislature.state.al.us/ALISON/SearchableInstruments/2016rs/PrintFiles/HB267-int.pdf.**
[5] *Available at*: **http://alisondb.legislature.state.al.us/ALISON/SearchableInstruments/2016rs/PrintFiles/HB291-int.pdf.**
[6] *Available at*: **http://alisondb.legislature.state.al.us/ALISON/SearchableInstruments/2016rs/PrintFiles/SB238-eng.pdf.**

## ALASKA

**STATUTE:** Alaska Stat. § **45.48.010** ***et seq.***[7]

### WHO MUST COMPLY?

Under § 45.48.010(a): a "covered person" 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.

### 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

[7] *Available at*: **http://www.legis.state.ak.us/basis/folioproxy.asp?url=http://wwwjnu01.legis.state.ak.us/cgi-bin/folioisa.dll/stattx09/query=%5bJUMP:'AS4548010'%5d/doc/%7b@1%7d?firsthit**.

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 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.

**WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?**

(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 (A) 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 (B) 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, (A) 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 v 45.48.010--45.48.090, except that the total civil penalty may not exceed $50,000; and (B) damages that may be awarded against the information collector under (i) § 45.50.531 are limited to actual economic damages that do not exceed $500; and (ii) § 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 INDUSTRY-SPECIFIC REQUIREMENTS?**

None.

## ARIZONA

**STATUTE:** Ariz. Rev. Stat. § **18-545** ***et seq.***[8]

### WHO MUST COMPLY?

Under § A, a person conducting business in Arizona that owns or licenses unencrypted computerized data that includes personal information must comply.

### WHAT DATA IS COVERED?

Under § L(6), personal information is covered. "Personal information" means:

(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 the data element is not encrypted, redacted or secured by any other method rendering the element unreadable or unusable:

(A) the individual's social security number;

(B) the individual's number on a driver license or number on a non-operating identification license;

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

### WHAT CONSTITUTES A DATA BREACH?

Under § L(1), "security breach" means an unauthorized acquisition of and access to unencrypted or unredacted computerized data that materially compromises the security or confidentiality of personal information maintained by a person as part of a database of personal information regarding multiple individuals and that causes or is reasonably likely to cause substantial economic loss to an individual.

"Security breach" does not include good faith acquisition of the information as defined by the statute.

### WHO MUST BE NOTIFIED?

Under § A, if an investigation results in a determination that there has been a breach in a security system, the individuals affected shall be notified.

### WHEN MUST NOTICE BE SENT?

[8] The Arizona legislature has not yet published the revised statute at the time of this Survey's publication.

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

**IN WHAT FORM AND MANNER MUST NOTICE BE SENT?**

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

(1) written notice;

(2) electronic notice if the person's primary method of communication with the individual is by electronic means or is consistent with statutory provisions;

(3) telephonic notice; 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 or that the affected class of subject individuals to be notified exceeds 100,000 persons, or the person does not have sufficient contact information.

Substitute notice shall consist of:

(A) Electronic mail notice if the person has electronic mail addresses for the individuals subject to the notice;

(B) Conspicuous posting of the notice on the web site of the person if the person maintains one; and

(C) 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.

**ARE THERE ANY EXEMPTIONS?**

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

Under § J, this section does not apply to either of the following:

(1) a person subject to title V of the Gramm-Leach-Bliley Act of 1999 (P.L. 106-102; 113 Stat. 1338; 15 U.S.C. §§ 6801 - 6809); or

(2) covered entities as defined under regulations implementing the Health Insurance Portability and Accountability Act ("HIPAA), 45 C.F.R. § 160.103 (1996).

## WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

Under § H, this section may only be enforced by the Attorney General. The Attorney General may bring an action to obtain actual damages for a willful and knowing violation of this section and a civil penalty not to exceed $10,000 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 INDUSTRY-SPECIFIC REQUIREMENTS?

None.

## ARKANSAS

**STATUTE:** Ark. Code § **4-110-101** ***et seq.***[9]

### WHO MUST COMPLY?

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

### WHAT DATA IS COVERED?

Under § 103(7), personal information is covered, meaning unencrypted or unredacted information consisting of an individual's personal information and any of the following:

(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; or

(4) medical information.

### WHAT CONSTITUTES A DATA BREACH?

Under § 103(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 §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 §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.

[9] *Available at*: http://www.lexisnexis.com/hottopics/arcode/Default.asp.

**IN WHAT FORM AND MANNER MUST NOTICE BE SENT?**

Under §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:

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

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

(C) 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 § 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.

**WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?**

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

**ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?**

None.

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

### WHAT DATA IS COVERED?

Under §§ 1798.29(g) and 1798.82(d), unencrypted personal information is covered. "Personal information" is defined as:

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

(A) social security number;

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

(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;

(E) health insurance information; 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.

### 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.

---

[10] *Available at*: **http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.25-1798.29**.

[11] *Available at*: **http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.80-1798.84**.

**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.

**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.

**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 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:

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

(B) conspicuous posting, for a minimum of 30 days, of the notice on the agency or business' Internet Web site page, if the agency maintains one; and

(C) notification to major statewide media and the Office of Information Security within the Department of Technology.

**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.

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

(A) The name and contact information of the reporting agency 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;

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

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

(B) 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.

**WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?**

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, 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 INDUSTRY-SPECIFIC REQUIREMENTS?**

Medical information statutes:

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.

## COLORADO

**STATUTE:** Colo. Rev. Stat. § **6-1-716**.[12]

### WHO MUST COMPLY?

Under § 716(2), an individual or a commercial entity that conducts business in Colorado and that owns or licenses computerized data that includes personal information about a resident of Colorado must comply.

### WHAT DATA IS COVERED?

Under § 716(2), computerized data that includes personal information about a resident of Colorado is covered.

"Personal information" means a Colorado resident's 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 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 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.

### WHAT CONSTITUTES A DATA BREACH?

Under § 716(1)(a), the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an individual or a commercial entity constitutes a data breach.

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.

### WHO MUST BE NOTIFIED?

Under § 716(2), Colorado residents must be notified.

Under § 716(2)(d), if an individual or commercial entity is required to notify more than 1,000

[12] *Available at*: **http://www.lexisnexis.com/hottopics/colorado/**.

Colorado residents of a breach of the security of the system pursuant to this section, the individual or commercial entity shall also notify, without unreasonable delay, 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 anticipated date of the notification to the residents and the approximate number of residents who are to be notified.

**WHEN MUST NOTICE BE SENT?**

Under § 716(2), 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.

**IN WHAT FORM AND MANNER MUST NOTICE BE SENT?**

Under § 716(c), notice may be provided in one of the following ways:

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

(2) telephonic notice;

(3) electronic notice, if a primary means of communication by the individual or commercial 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 15 U.S.C. §§ 7001 *et seq.*; or

(4) substitute notice, if the individual or the commercial 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 individual or the commercial entity does not have sufficient contact information to provide notice.

Substitute notice consists of all of the following:

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

(B) 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 one; and

(C) 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.

**ARE THERE ANY EXEMPTIONS?**

Under § 716(c), 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 individual or commercial entity that conducts business in Colorado not to send notice.

**WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?**

Under § 716(4), the Attorney General may bring an action in law or 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.

**ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?**

None.

## CONNECTICUT

**STATUTE:** Conn. Gen. Stat. § **36a-701b**,[13] **2015 S.B. 949, Public Act 15-142**.[14]

### 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.

### WHAT DATA IS COVERED?

Under § 36a-701b(a), personal information is covered. "Personal information" means an individual's name in combination with any one, or more, of the following data:

(1) social security number;

(2) driver's license number or state 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.

### 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 must be notified.

### WHEN MUST NOTICE BE SENT?

Under § 36a-701b(b)(1), notice shall be made without unreasonable delay, 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

[13] *Available at*: **http://law.justia.com/codes/connecticut/2012/title-36a/chapter-669/section-36a-701b**
[14] *Available at*: **https://www.cga.ct.gov/2015/ACT/PA/2015PA-00142-R00SB-00949-PA.htm**.

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 Web site 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?**

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

**ARE THERE ANY EXEMPTIONS?**

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.

**WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?**

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.

## ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

None.

## DELAWARE

**STATUTE:** Del. Code tit. 6, §§ **12B-101** ***et seq.***[15]

### WHO MUST COMPLY?

Under § 12B-102(a), an individual or a commercial entity that conducts business in Delaware and that owns or licenses computerized data that includes personal information about a resident of Delaware must comply.

### WHAT DATA IS COVERED?

Under § 12B-102(a), personal information is covered. Under § 12B-101(4), "personal information" means a Delaware resident's 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:

(A) social Security number;

(B) driver's license number or Delaware Identification Card number; or

(C) 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.

The term "personal information" does not, however, 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 § 12B-101(1), a data breach consists of the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an individual or a commercial entity.

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

### WHO MUST BE NOTIFIED?

Under § 12B-102(a), an individual or a commercial entity that conducts business in Delaware and that owns or licenses computerized data that includes personal information about a resident of Delaware shall, when it becomes aware of a breach of the security of the system, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused. If the investigation determines that the misuse of

[15] *Available at*: **http://delcode.delaware.gov/title6/c012b/index.shtml**.

information about a Delaware resident has occurred or is reasonably likely to occur, the individual or the commercial entity shall give notice as soon as possible to the affected Delaware resident.

Under § 12B-102(b), 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 shall give notice to and cooperate with the owner or licensee of the information of any breach of the security of the system immediately following discovery of a breach, if misuse of personal information about a Delaware resident occurred or is reasonably likely to occur.

**WHEN MUST NOTICE BE SENT?**

Under § 12B-102(a), notice must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.

**IN WHAT FORM AND MANNER MUST NOTICE BE SENT?**

Under § 12B-101(3), 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

(4) substitute notice, if the individual or the commercial entity required to provide notice demonstrates that the cost of providing notice will exceed $75,000 or that the affected class of Delaware residents to be notified exceeds 100,000 residents, or that the individual or the commercial entity does not have sufficient contact information to provide notice.

Substitute notice consists of all of the following:

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

(B) 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 one; and

(C) 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 § 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. Notice required by this chapter must 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.

**WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?**

Under §12B-104, 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 an individual or a commercial entity subject to this chapter from compliance with all other applicable provisions of law.

**ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?**

None.

## DISTRICT OF COLUMBIA

**STATUTE:** D.C. Code §§ **28-3851** ***et seq.***[16]

### WHO MUST COMPLY?

Under § 18-3852(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. 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 § 18-3852(a) and (b), personal information is covered. Under § 28-3851(3)(A), "personal information" means:

(1) 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:

(A) social security number;

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

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

(D) any other number or code 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. 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.

[16] *Available at*: **http://www.lexisnexis.com/hottopics/dccode/**.

**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.

**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.

Under § 28-3852(b), notice shall be made in the most expedient time possible following discovery of a breach.

**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, approved June 30, 2000; 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:

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

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

(C) 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(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.

**WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?**

Under § 28-3853, 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. Additionally, any District of Columbia resident injured by a violation of this subchapter may institute a civil action to recover actual damages, the costs of the action, and reasonable attorney's fees.

The Attorney General may 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**,[17] **282.0041**,[18] **282.318(2)(i)**.[19]

### WHO MUST COMPLY?

Under § 501.171(4), covered entities must comply. Under § 501.171(1)(b), "covered entities" 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 in subsections (3)-(6), the term includes a governmental entity.

### WHAT DATA IS COVERED?

Under § 501.171(4), personal information is covered. "Personal information" consists of an individual's name and either:

(1) social security number;

(2) driver's license or state ID number; or

(3) information that would allow access to financial accounts.

### 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.

---

[17] *Available at*:
**http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=0500-0599/0501/Sections/0501.171.html**.
[18] *Available at*:
**http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=0200-0299/0282/Sections/0282.0041.html**.
[19] *Available at*:
**http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=0200-0299/0282/Sections/0282.318.html**.

**WHEN MUST NOTICE BE SENT?**

Under § 501.171(4)(a), notice must be sent as expeditiously as practicable and without unreasonable delay, but no later than 30 days after the determination of a breach or reason to believe a 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;

(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 if the person or business providing the notice has a valid email address for the subject person and the subject person has agreed to accept communications electronically; or

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

Substitute notice shall include the following:

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

(B) 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 email 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.

**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.

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.

**WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?**

Under § 501.171(9)(a), the Florida Department of Legal Affairs may enforce this section. 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 INDUSTRY-SPECIFIC REQUIREMENTS?**

None.

## GEORGIA

**STATUTE:** Ga. Code §§ **10-1-910, -911, -912; § 46-5-214**[20]

### 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.

### 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 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 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.

[20] *Available at*: **http://www.lexisnexis.com/hottopics/gacode/Default.asp**.

**WHO MUST BE NOTIFIED?**

Under § 10-1-912(a) and (b), 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(d), 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), shall be notified of the timing, distribution and content of the notices in the event that the information broker or data collector discovers circumstances requiring notification pursuant to this Code section of more than 10,000 resident of Georgia at one time.

**WHEN MUST NOTICE BE SENT?**

Under § 10-1-912(a), notice shall be made in the most expedient time possible and without unreasonable delay, except as necessary for law enforcement purposes or to determine the scope of the breach and restore the integrity, security, and confidentiality of the information system.

**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:

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

(B) 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

(C) 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.

**ARE THERE ANY EXEMPTIONS?**

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?**

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.

**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.

## GUAM

**STATUTE:** 9 GCA § **48-10** ***et seq.***[21]

### WHO MUST COMPLY?

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

### WHAT DATA IS COVERED?

Under § 48.30(a), personal information is covered. Under § 48.20(f), "personal information" means unencrypted information consisting of an individual's name with any one or more of the following:

(1) social Security number;

(2) driver's license number of 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 passwords 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.

### 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.

### 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 must be notified.

### WHEN MUST NOTICE BE SENT?

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

[21] *Available at*: **http://www.guamcourts.org/compileroflaws/GCA/09gca/9gc048.pdf**.

**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:

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

(B) 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

(C) 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.

**WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?**

Under § 48.50(a), a violation of this chapter 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 INDUSTRY-SPECIFIC REQUIREMENTS?**

None.

## HAWAII

**STATUTE:** Haw. Rev. Stat. § **487N-1** ***et seq.***[22]

### 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.

### WHAT DATA IS COVERED?

Under § 487N-2(a), personal information is covered. Under § 487N-1, "personal information" means a person's name in combination with any one or more of the following:

(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.

### 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.

### 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.

### WHEN MUST NOTICE BE SENT?

Under § 487N-1, notice shall be made without unreasonable delay, consistent with the legitimate

[22] *Available at*: **http://www.capitol.hawaii.gov/hrscurrent/Vol11_Ch0476-0490/HRS0487N/HRS_0487N-0001.htm**.

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.

**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:

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

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

(C) notification to major statewide media.

**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.

**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.

**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 INDUSTRY-SPECIFIC REQUIREMENTS?**

None.

## IDAHO

**STATUTE:** Idaho Stat. § **28-51-104 to -107**.[23]

**WHO MUST COMPLY?**

Under § 28-51-105, agencies, individuals or commercial entities must comply.

**WHAT DATA IS COVERED?**

Under § 28-51-105, personal information is covered. Under §28-51-104(5), "personal information" means an Idaho resident's 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.

**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, an affected Idaho resident must be notified.

**WHEN MUST NOTICE BE SENT?**

Under § 28-51-105, notice must be given as soon as possible and in the most expedient time possible, without unreasonable delay.

[23] *Available at*: **http://www.legislature.idaho.gov/idstat/Title28/T28CH51.htm**.

**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:

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

(B) 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

(C) 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.

**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 INDUSTRY-SPECIFIC REQUIREMENTS?

None.

## ILLINOIS

**STATUTE:** 815 ILCS § **530/1-530/25**.[24]

### WHO MUST COMPLY?

Under 815 ILCS § 530/10, any data collector that owns or licenses personal information concerning an Illinois resident. "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.

### WHAT DATA IS COVERED?

Personal information is covered. Under 815 ILCS § 530/5, "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.

(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.

"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 ILCS § 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.

---

[24] *Available at*: **http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=2702&ChapAct=815 ILCS 530/&ChapterID=67&ChapterName=BUSINESS+TRANSACTIONS&ActName=Personal+Information+Protection+Act**.

**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..

**IN WHAT FORM AND MANNER MUST NOTICE BE SENT?**

Notice to consumers 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:

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

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

(C) notification to major statewide media.

**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.

**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.

**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. If an individual can show actual damages, he or she may be able to sue for a violation of the Act. *See Cooney v. Chicago Public Schools*, 407 Ill. App. 3d 358 (Ill. Ct. App. 2010).

**ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?**

None.

## INDIANA

**STATUTE:** Ind. Code §§ **4-1-11 *et seq.*, 24-4.9 *et seq.***[25]

### WHO MUST COMPLY?

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

### WHAT DATA IS COVERED?

"Personal information," meaning:

Under § 4-1-11-3, applicable to State Agencies, information consisting of an individual's 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.

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 name 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.

### 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 state or local

[25] *Available at*: **https://iga.in.gov/legislative/laws/2015/ic/**.

agency.

The term does not include the following:

(1) the good faith acquisition of personal information by an agency or employee of the agency for purposes of the 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.

**WHO MUST BE NOTIFIED?**

Any state resident 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?**

Notice must be sent without unreasonable delay.

**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.

**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.

**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 $150,000 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 INDUSTRY-SPECIFIC REQUIREMENTS?**

None.

## IOWA

**STATUTE:** Iowa Code §§ **715C.1**,[26] **715C.2**.[27]

### 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.

### 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, unredact, 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 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

(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

[26] *Available at*: https://coolice.legis.iowa.gov/cool-ice/default.asp?category=billinfo&service=iowacode&ga=83&input=715C.
[27] *Available at*: https://coolice.legis.iowa.gov/cool-ice/default.asp?category=billinfo&service=iowacode&ga=83&input=715C.

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.

**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.

**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:

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

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

(C) 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.

**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.

**ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?**

None.

## KANSAS

**STATUTE:** Kan. Stat. § **50-7a01** ***et seq.***[28]

### 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.

### WHAT DATA IS COVERED?

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.

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, 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, without unreasonable

[28] *Available at*:
**http://www.kslegislature.org/li_2014/b2013_14/statute/050_000_0000_chapter/050_007a_0000_article/**.

delay, 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.

**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:

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

(B) 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

(C) 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.

**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.

**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 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.

## KENTUCKY

**STATUTE:** K.R.S. §§ **365.732**,[29] **61.931-61.934**.[30]

### WHO MUST COMPLY?

A person or business entity that conducts business in the state and which owns, licenses, or maintains computerized data which includes personal information about a Kentucky resident. K.R.S. § 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. K.R.S. § 365.732(1)(c).

### WHAT CONSTITUTES A DATA BREACH?

Unauthorized acquisition of unencrypted and unredacted computerized data that compromises the security, confidentiality, or integrity of personally identifiable information maintained by the information holder as part of a database regarding multiple individuals that actually causes, or leads the information holder to reasonably believe 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. K.R.S. § 365.732(1)(a).

The statute does not apply if the data subject to the breach is encrypted or redacted. 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. K.R.S. § 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. K.R.S. § 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 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. K.R.S. § 365.732(7).

---

[29] *Available at*: **http://www.lrc.ky.gov/Statutes/statute.aspx?id=43326**.
[30] *Available at*: **http://www.lrc.ky.gov/Statutes/statute.aspx?id=43575**.

**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. K.R.S. § 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:

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

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

(C) notification to major statewide media. K.R.S. § 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. K.R.S. § 365.732(6).

The provisions of this section and the requirements for non-affiliated third-parties in K.R.S. 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. K.R.S. § 365.732(8).

**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.

**ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?**

None.

## LOUISIANA

**STATUTE:** La. Rev. Stat. §§ **51:3071 *et seq.***,[31] **40:1173.1-40:1173.6**.[32]

### WHO MUST COMPLY?

Any person or agency that conducts business in the state or that owns, maintains or licenses computerized data that includes personal information regarding a Louisiana resident. La. Rev. Stat. §§ 51:3074(A), 51:3074(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 element is not encrypted or redacted:

(A) social security number;

(B) driver's license number; or

(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.

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).

### WHAT CONSTITUTES A DATA BREACH?

The compromise of the security, confidentiality, or integrity of computerized data that results in, or there is a reasonable basis to conclude has resulted in, the unauthorized acquisition of and access to personal information maintained by an agency or person. 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 the state whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person. La. Rev. Stat. § 51: 3074(A).

If the breach affects a person that maintains or stores covered information, that person must notify the owner or licensee of that information. La. Rev. Stat. § 51:3074(B).

### WHEN MUST NOTICE BE SENT?

The notification shall be made in the most expedient time possible and without unreasonable

[31] *Available at*: **http://legis.la.gov/Legis/Law.aspx?d=322030**.
[32] *Available at*: **http://legis.la.gov/Legis/Law.aspx?d=964730**.

delay, consistent with the legitimate needs of law enforcement, or any measures necessary to determine the scope of the breach, prevent further disclosures, and restore the reasonable integrity of the data system. La. Rev. Stat. § 51:3074(C).

**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 an agency or person demonstrates that the cost of providing notification would exceed $250,000, or that the affected class of persons to be notified exceeds 500,000, or the agency or person does not have sufficient contact information.

Substitute notification shall consist of all of the following:

(A) email notification when the agency or person has an email address for the subject persons;

(B) conspicuous posting of the notification on the Internet site of the agency or person, if an Internet site is maintained; and

(C) notification to major statewide media. La. Rev. Stat. § 51:3074(E).

**WHAT MUST THE NOTICE SAY?**

The statute does not address the contents of the notification.

**ARE THERE ANY EXEMPTIONS?**

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 this section shall be deemed to be in compliance with the notification requirements of this section if the agency or person notifies subject persons in accordance with the policy and procedure in the event of a breach of security of the system. La. Rev. Stat. § 51:3074(F).

Notification under this section is not required if after a reasonable investigation the person or business determines that there is no reasonable likelihood of harm to customers. La. Rev. Stat. § 51:3074(G).

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.

Notification under the statute is not required if after a reasonable investigation the person or business determines that there is no reasonable likelihood of harm to customers. La. Rev. Stat. § 51:3074(G).

**WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?**

A private civil action may be instituted to recover actual damages resulting from the failure to disclose in a timely manner to a person that there has been a breach of the security system resulting in the disclosure of a person's personal information. La. Rev. Stat. § 51:3075.

**ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?**

The Department of Health and Hospitals must comply with §§ 40:1173.1 to 40:1173.6, which requires the Department to notify, within thirty days of the breach, each resident of the state whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

## MAINE

**STATUTE:** Me. Rev. Stat. tit. 10 § **1346** ***et seq.***[33]

### WHO MUST COMPLY?

A person who, for monetary fees or dues, engages in whole or in part in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring or communicating information concerning 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. 10 M.R.S.A. §§ 1347(3), 1347(5).

### 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:

(A) social security number;

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

(C) 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;

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

(E) any of the data elements contained in paragraphs (a) to (d) 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. 10 M.R.S.A. § 1347(6).

### 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

[33] *Available at*: **http://legislature.maine.gov/statutes/10/title10ch210-Bsec0.html**.

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. 10 M.R.S.A. § 1347(1).

**WHO MUST BE NOTIFIED?**

Any affected resident of this State if misuse of the personal information has occurred or if it is reasonably possible that misuse will occur. 10 M.R.S.A. § 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. 10 M.R.S.A. § 1348(2).

When notice of a breach of the security of the system is required under subsection (1), 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. 10 M.R.S.A. § 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. 10 M.R.S.A. § 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 pursuant to subsection (3) 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. 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. 10 M.R.S.A. § 1348(3).

**IN WHAT FORM AND MANNER MUST NOTICE BE SENT?**

The notice must be: (a) written notice; (b) 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 (c) 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) email notice, if the person has email 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. 10 M.R.S.A. § 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 law of this State 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 the notification requirements of § 1348. 10 M.R.S.A. § 1349(4).

**WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?**

The appropriate State regulators within the Department of Professional and Financial Regulation shall enforce this chapter for any person that is licensed or regulated by those regulators. The Attorney General shall enforce this chapter for all other persons. 10 M.R.S.A. § 1349(1).

A person that violates this chapter commits a civil violation and is subject to one or more of the following: (a) a fine of not more than $500 per violation, up to a maximum of $2,500 for each day the person is in violation of this chapter, except that this paragraph does not apply to State Government, the University of Maine System, the Maine Community College System or Maine Maritime Academy; (b) equitable relief; or (c) enjoinment from further violations of this chapter. 10 M.R.S.A. § 1349(2).

The rights and remedies available under this section are cumulative and do not affect or prevent rights and remedies available under federal or State law. 10 M.R.S.A. § 1349(3).

**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 § **14-3501** ***et seq.***, Md. State Govt. Code §§ **10-1301-1308**.[34]

### WHO MUST COMPLY?

A business that owns, maintains or licenses computerized data that includes personal information of an individual residing in Maryland. Md. Code, Commercial Law §§ 14-3504(b), 14-3504(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 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:

(A) social security number;

(B) driver's license number;

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

(D) individual taxpayer identification number.

Personal information does not include: (i) publicly available information that is lawfully made available to the general public from federal, State, or local government records; (ii) information that an individual has consented to have publicly disseminated or listed; or (iii) information that is disseminated or listed in accordance with the federal Health Insurance Portability and Accountability Act ("HIPAA"). Md. Code, Commercial Law § 14-3501(d).

### 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, Commercial Law § 14-3504(a).

The statute does not apply if the data subject to the breach 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, Commercial Law § 14-3501(c).

[34] *Available at*: **http://www.lexisnexis.com/hottopics/mdcode/**.

**WHO MUST BE NOTIFIED?**

If, after the investigation is concluded, the business determines that misuse of the individual's personal information has occurred or is reasonably likely to occur as a result of a breach of the security of a system, the business shall notify the individual of the breach. Prior to providing notice to an individual, a business shall first provide notice of a breach of the security of a system to the Office of the Attorney General. Md. Code, Commercial Law § 14-3504(b).

If the breach affects a person that maintains or stores covered information, that person must notify the owner or licensee of that information. Md. Code, Commercial 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. Md. Code, Commercial Law § 14-3506(a).

**WHEN MUST NOTICE BE SENT?**

Notification shall be given as soon as reasonably practicable after the business discovers or is notified of the breach of the security of a system or as soon as reasonably practicable after the law enforcement agency determines that it will not impede a criminal investigation and will not jeopardize homeland or national security. Md. Code, Commercial Law § 14-3504(b).

**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:

(i) the individual has expressly consented to receive electronic notice; or

(ii) 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: (i) 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 (ii) The business does not have sufficient contact information to give notice in accordance with item (a), (b), or (c) of this subsection.

Substitute notice shall consist of: (1) electronically mailing the notice to an individual entitled to notification, if the business has an electronic mail address for the individual to be notified;

(2) conspicuous posting of the notice on the Web site of the business, if the business maintains a Web site; and (3) notification to statewide media. Md. Code, Commercial Law § 14-3504(e).

**WHAT MUST THE NOTICE SAY?**

The notification shall include:

(1) to the extent possible, a description of the categories of information that were, or are reasonably believed to have been, acquired by an unauthorized person, including which of the elements of personal information were, or are reasonably believed to have been, acquired;

(2) contact information for the business making the notification, including the business' address, telephone number, and toll-free telephone number if one is maintained;

(3) the toll-free telephone numbers and addresses for the major consumer reporting agencies; and

(4) (i) the toll-free telephone numbers, addresses, and Web site addresses for: (1) the Federal Trade Commission; and (2) the Office of the Attorney General; and (ii) a statement that an individual can obtain information from these sources about steps the individual can take to avoid identity theft. Md. Code, Commercial Law § 14-3504(g).

**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 this subtitle.

A business or affiliate that is subject to and in compliance with § 501(b) of the federal Gramm-Leach-Bliley Act, 15 U.S.C. § 6801, § 216 of the federal Fair and Accurate Credit Transactions Act, 15 U.S.C. § 1681w, the federal Interagency Guidelines Establishing Information Security Standards, and the federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, and any revisions, additions, or substitutions thereof, shall be deemed to be in compliance with this subtitle. Md. Code, Commercial Law § 14-3507.

**WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?**

The Attorney General may seek an injunction to prohibit a person who has engaged or is engaging in a violation of this title from continuing or engaging in the violation.

(A) The Attorney General shall serve notice of the general relief sought on the alleged violator at least seven days before the action for an injunction is filed.

(B) The court may enter any order of judgment necessary to:

(1) prevent the use by a person of any prohibited practice;

(2) restore to a person any money or real or personal property acquired from him by means of any prohibited practice; or

(3) appoint a receiver in case of willful violation of this title. Md. Code, Commercial Law § 13-406.

There is a private right of action for violations of the statute. Any person who brings an action to recover for injury or loss under this section and who is awarded damages may also seek, and the court may award, reasonable attorney's fees. If it appears to the satisfaction of the court, at any time, that an action is brought in bad faith or is of a frivolous nature, the court may order the offending party to pay to the other party reasonable attorney's fees. Md. Code, Commercial Law § 13-408.

In any action brought by the Attorney General under the provisions of this title, the Attorney General is entitled to recover the costs of the action for the use of the State. Md. Code, Commercial Law § 13-409.

A merchant who violates the statute is subject to a fine of not more than $1,000 for each violation. A merchant who has been found to have engaged in a violation of this title and who subsequently repeats the same violation is subject to a fine of not more than $5,000 for each subsequent violation. The fines provided for in this section are civil penalties and are recoverable by the State in a civil action or an administrative cease and desist action under § 13-403(a) and (b) of this subtitle or after an administrative hearing has been held under § 13-403(d)(3) and (4) of this subtitle. The Consumer Protection Division shall consider the following in setting the amount of the penalty imposed in an administrative proceeding:

(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, Commercial 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, Commercial Law § 13-411.

**ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?**

None.

## MASSACHUSETTS

**STATUTE:** Mass. Gen. Laws § **93H-1** ***et seq.***[35]

### WHO MUST COMPLY?

A person or agency that maintains, stores, owns, or licenses data that includes personal information about a resident of the commonwealth. M.G.L. 93H § 3(a), (b).

### 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; provided, however, that "personal information" shall 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. M.G.L. 93H § 1.

### 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 the commonwealth. A good faith but unauthorized acquisition of personal information by a person or agency, or employee or agent thereof, for the lawful purposes of such person or agency, is not a breach of security unless the personal information is used in an unauthorized manner or subject to further unauthorized disclosure. M.G.L. 93H § 1(a).

The statute does not apply to data that is encrypted. "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, unless further defined by regulation of the Department of Consumer Affairs and Business Regulation. M.G.L. 93H § 1(a).

### WHO MUST BE NOTIFIED?

A person or agency that owns or licenses data that includes personal information about a resident of the commonwealth shall provide notice to the Attorney General, the Director of Consumer

[35] *Available at*: **https://malegislature.gov/Laws/GeneralLaws/PartI/TitleXV/Chapter93h/Section1**.

Affairs and Business Regulation, and to such resident.

A person that maintains or stores data that includes personal information shall provide notice to the owner or licensee of that data. M.G.L. 93H § 3(a).

**WHEN MUST NOTICE BE SENT?**

A person responsible to send notice must do so as soon as practicable, and without unreasonable delay, following (1) discovery of a breach of security, or (2) when the person or agency knows or has reason to know that the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose, except as necessary for a criminal investigation by a law enforcement agency. M.G.L. 93H § 3(a), (b).

**IN WHAT FORM AND MANNER MUST NOTICE 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: (i) electronic mail notice, if the person or agency has electronic mail addresses for the members of the affected class of Massachusetts residents; (ii) 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 (iii) publication in, or broadcast through, media or medium that provides notice throughout the commonwealth. M.G.L. 93H § 3(a).

**WHAT MUST THE NOTICE SAY?**

The notice shall include, but not be limited to, the consumer's right to obtain a police report, how a consumer requests a security freeze and the necessary information to be provided when requesting the security freeze, and any fees required to be paid to any of the consumer reporting agencies; provided, however, that the notification shall not include the nature of the breach or unauthorized acquisition or use or the number of residents of the commonwealth affected by the breach or unauthorized access or use. M.G.L. 93H § 3(a).

**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 this chapter. M.G.L. 93H § 5.

**WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?**

The Attorney General may bring an action pursuant to § 4 of chapter 93A against a person or otherwise to remedy violations of this chapter and for other relief that may be appropriate. M.G.L. 93H § 6.

Under M.G.L. 93A § 4, if the court finds that a person has employed any method, act or practice which he knew or should have known to be in violation of section (2), the court may require such person to pay to the commonwealth a civil penalty of not more than $5,000 for each such violation and also may require the person to pay the reasonable costs of investigation and litigation of such violation, including reasonable attorneys' fees.

There is no private right of action. M.G.L. 93A § 4.

**ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?**

None.

## MICHIGAN

**STATUTE:** Mich. Comp. Laws §§ **445.63**,[36] **445.72**.[37]

### WHO MUST COMPLY?

A person or agency that owns, maintains or licenses data which includes personal information of a resident of the State, that are included in a database. M.C.L.A. **§** 445.72(1).

### 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 resident of this state:

(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. M.C.L.A. **§** 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: (a) the employee or other individual acted in good faith in accessing the data; (b) the access was related to the activities of the agency or person; and (c) the employee or other individual did not misuse any personal information or disclose any personal information to an unauthorized person. M.C.L.A. **§** 445.63(b).

The statute does not apply if the data subject to the breach is encrypted. This exception does not apply if the encryption is compromised. Encryption 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 information by another method that renders the data elements unreadable or unusable. M.C.L.A. **§** 445.63(g).

### WHO MUST BE NOTIFIED?

Each resident of the State who meets one or more of the following:

---

[36] *Available at*: http://www.legislature.mi.gov/(S(mage2kx0gy2fpanhe00tqzmx))/mileg.aspx?page=GetObject&objectname=mcl-445-63.

[37] *Available at*: http://www.legislature.mi.gov/(S(mage2kx0gy2fpanhe00tqzmx))/mileg.aspx?page=GetObject&objectname=mcl-445-72.

(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. M.C.L.A. § 445.72(1).

If the breach affects a person that maintains or stores covered information, that person must notify the owner or licensee of that information. M.C.L.A. § 445.72(2).

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. This subsection does not apply if either of the following is met: (a) the person or agency is required under this section to provide notice of a security breach to 1,000 or fewer residents of this state; or (b) the person or agency is subject to 15 U.S.C. §§ 6801 to 6809.

**WHEN MUST NOTICE BE SENT?**

Notice should be sent without unreasonable delay, except as necessary to determine the scope of the security breach, restore the reasonable integrity of the database, and as necessary for law enforcement purposes. M.C.L.A. § 445.72(4).

**IN WHAT FORM AND MANNER MUST NOTICE BE SENT?**

An agency or person shall provide any notice required under this section 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 (consistent with the statute's provisions);

(3) notice given by telephone by an individual who represents the person or agency (consistent with the statute's provisions);

(4) substitute notice, if the person or agency demonstrates that the cost of providing notice under subdivision (a), (b), or (c) will exceed $250,000.00 or that the person or agency has to provide notice to more than 500,000 residents of the State.

A person or agency provides substitute notice under this subdivision by doing all of the following:

(i) if the person or agency has electronic mail addresses for any of the residents of the State who are entitled to receive the notice, providing electronic notice to those residents;

(ii) if the person or agency maintains a website, conspicuously posting the notice on that website; and

(iii) notifying major statewide media. A notification under this subparagraph shall include a telephone number or a website address that a person may use to obtain additional assistance and information. M.C.L.A. § 445.72(5).

**WHAT MUST THE NOTICE SAY?**

The notice must: (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. M.C.L.A. § 445.72(6).

**ARE THERE ANY EXEMPTIONS?**

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 section. M.C.L.A. § 445.72(10).

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 section. M.C.L.A. § 445.72(9).

This section applies to the discovery or notification of a breach of the security of a database that occurs on or after July 2, 2006. M.C.L.A. § 445.72(16).

This section 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. M.C.L.A. § 445.72(17).

**WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?**

The Attorney General or a prosecuting attorney may bring an action to recover a civil fine under this section. A person that knowingly fails to provide any notice of a security breach required under this section may be ordered to pay a civil fine of not more than $250 for each failure to provide notice. The aggregate liability of a person for civil fines for multiple violations that arise from the same security breach shall not exceed $750,000.

There is a private right of action under the statute. M.C.L.A. § 445.72(15).

## 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 manner described in subsection (5), or alternatively by providing all of the following:

(1) as applicable, notice as described in subsection (5)(b);

(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; and

(4) 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. M.C.L.A. **§** 445.72(11).

## MINNESOTA

**STATUTE:** Minn. Stat. Ann. §§ **325E.61**,[38] **325E.64**.[39]

### WHO MUST COMPLY?

Any person or business that conducts business in the State, and that owns, maintains, or licenses data that includes personal information must disclose the breach to affected residents of the State. M.S.A. § 325E.61(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 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. M.S.A. § 325E.61(1).

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?

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 personal information is not used or subject to further unauthorized disclosure.

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. M.S.A. § 325E.61(1).

### WHO MUST BE NOTIFIED?

Any resident of the State whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. M.S.A. § 325E.61(1).

If the breach affects a person that maintains or stores covered information, that person must notify the owner or licensee of that information. M.S.A. § 325E.61(1).

---

[38] *Available at*: **https://www.revisor.mn.gov/statutes/?id=325E.61**.
[39] *Available at*: **https://www.revisor.mn.gov/statutes/?id=325E.64**.

If a person discovers circumstances requiring notification under this section and § 13.055(6) 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, as defined by 15 U.S.C. § 1681a, of the timing, distribution, and content of the notices. M.S.A. § 325E.61(2).

**WHEN MUST NOTICE BE SENT?**

Notification must occur immediately following discovery of the breach, except as necessary for a criminal investigation by law enforcement. M.S.A. § 325E.61(1).

**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 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 or business does not have sufficient contact information.

Substitute notice must consist of all of the following:

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

(ii) conspicuous posting of the notice on the Web site page of the person or business, if the person or business maintains one; and

(iii) notification to major statewide media. M.S.A. § 325E.61(1).

**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). M.S.A. § 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 this section and § 13.055(6) shall be deemed to be in compliance with the notification requirements of this section and § 13.055(6) if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system. M.S.A.

§ 325E.61(1).

**WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?**

The Attorney General shall enforce this statute under Minnesota's Unfair Trade Practices statute, and may seek injunctive relief an monetary penalties up to $25,000. M.S.A. § 8.31.

**ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?**

M.S.A. § 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.

No person or entity conducting business in Minnesota that accepts an access device 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 of this section if its service provider retains such 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.

Whenever there is a breach of the security of the system of a person or entity that has violated this section, 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.

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 this section. Costs do not include any amounts recovered from a credit card company by a financial institution. The remedies under this subdivision are cumulative and do not restrict any other right or remedy otherwise available to the financial institution. M.S.A. § 325E64.

## MISSISSIPPI

**STATUTE:** Miss. Code § **75-24-29**.[40]

### WHO MUST COMPLY?

Any person who conducts business in the State and who, in the ordinary course of the person's business functions, owns, licenses or maintains personal information of any resident of the State. Miss. Code § 75-24-29(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:

(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).

### WHAT CONSTITUTES A DATA BREACH?

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

The statute does not apply if the data subject to the breach is secured by encryption or by any other method or technology that renders the personal information unreadable or unusable. Miss. Code § 75-24-29 (2).

### WHO MUST BE NOTIFIED?

Any individual who is a resident of the State 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(3).

If the breach affects a person that maintains or stores covered information, that person must notify the owner or licensee of that information. Miss. Code § 75-24-29(4).

[40] *Available at*: **http://www.lexisnexis.com/hottopics/mscode/**.

**WHEN MUST NOTICE BE SENT?**

The disclosure 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(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: (a) written notice; (b) telephone notice; (c) 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 (d) substitute notice, provided the person demonstrates that the cost of providing notice in accordance with paragraph (a), (b) or (c) of this subsection would exceed $5,000.00, that the affected class of subject persons to be notified exceeds 5,000 individuals, or the person does not have sufficient contact information.

Substitute notice shall consist of the following: (1) electronic mail notice when the person has an electronic mail address for the affected individuals; (2) conspicuous posting of the notice on the Web site of the person if the person maintains one; and (3) notification to major statewide media, 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 the State that maintains its own security breach procedures as part of an information security policy for the treatment of personal information, and otherwise complies with the timing requirements of this section, shall be deemed to be in compliance with the security breach notification requirements of this section 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 this section, 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 Attorney General may enforce this statute. Failure to comply with the requirements of this section shall constitute an unfair trade practice. However, nothing in this section may be construed to create a private right of action. Miss. Code § 75-24-29(8).

## ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

None.

## MISSOURI

**STATUTE:** Mo. Rev. Stat. § **407.1500**.[41]

### WHO MUST COMPLY?

Any person that maintains, possesses, owns, or licenses records or data containing personal information of residents of Missouri. Mo. Rev. Stat. § 407.1500(2).

### 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 information; or

(6) health insurance information.

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).

### WHAT CONSTITUTES A DATA BREACH?

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

[41] *Available at*: **http://www.moga.mo.gov/mostatutes/stathtml/40700015001.html**.

The statute does not apply if the data subject to the breach encrypted, redacted, or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable or unusable. Mo. Rev. Stat. § 407.1500(1).

**WHO MUST BE NOTIFIED?**

Missouri residents whose data is affected. 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).

In the event a person provides notice to more than 1,000 consumers at one time pursuant to this section, the person shall notify, without unreasonable delay, the Attorney General's office 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), of the timing, distribution, and content of the notice. Mo. Rev. Stat. § 407.1500(2).

**WHEN MUST NOTICE BE SENT?**

Notice must be made without unreasonable delay, immediately following the discovery of the breach, except as necessary for law enforcement purposes and as necessary to determine sufficient contact information and determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system. Mo. Rev. Stat. § 407.1500(2).

**IN WHAT FORM AND MANNER MUST NOTICE BE SENT?**

Notice to affected consumers 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 email 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 (a), (b), or (c) of this subdivision, 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.

Substitute notice shall consist of all the following: (a) email notice when the person has an electronic mail address for the affected consumer; (b) conspicuous posting of the notice or a link to the notice on the internet website of the person if the person maintains an internet website; and (c) notification to major statewide media. Mo. Rev. Stat. § 407.1500(2).

**WHAT MUST THE NOTICE SAY?**

The notice shall 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).

**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, 15 U.S.C. §§ 6801 to 6809. Mo. Rev. Stat. § 407.1500(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 this section, is deemed to be in compliance with the notice requirements of this section if the person notifies affected consumers in accordance with its policies in the event of a breach of security of the system. Mo. Rev. Stat. § 407.1500(3).

A person that is regulated by state or federal law and that maintains procedures for a breach of the security of the system pursuant to the laws, rules, regulations, guidances, or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance with this section if the person notifies affected consumers in accordance with the maintained procedures when a breach occurs. Mo. Rev. Stat. § 407.1500(3).

**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 and may seek a civil penalty not to exceed 150,000 per breach of the security of the system or series of breaches of a similar nature that are discovered in a single investigation. Mo. Rev. Stat. § 407.1500(4).

**ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?**

None.

## MONTANA

**STATUTE:** Mont. Code §§ **2-6-1501-1503**,[42] **30-14-1701 *et seq.***,[43] **33-19-321**.[44]

### WHO MUST COMPLY?

Any person or business that conducts business in Montana and that owns, maintains, or licenses computerized data that includes personal information. Any state agency that maintains computerized data containing personal information in the data system. Mont. Code § 30-14-1704(1).

### WHAT DATA IS COVERED?

A 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 number, state identification card number, 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 as defined in § 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 from federal, state, local, or tribal government records. Mont. Code § 30-14-1704(4).

### 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 § 30-14-1704(4).

The statute does not apply if the data subject to the breach is encrypted. The statute does not

[42] *Available at*: **http://leg.mt.gov/bills/mca_toc/2_6_15.htm**.
[43] *Available at*: **http://leg.mt.gov/bills/mca_toc/30_14_17.htm**.
[44] *Available at*: **http://leg.mt.gov/bills/mca/33/19/33-19-321.htm**.

define encryption. Mont. Code § 30-14-1704(1).

**WHO MUST BE NOTIFIED?**

Any individual whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. Mont. Code § 30-14-1704(1).

If the breach affects a person or agency that maintains or stores covered information, that person must notify the owner or licensee of that information. Mont. Code § 30-14-1704(2).

Any person or business 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 Attorney General's consumer protection office, 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 § 30-14-1704(8).

**WHEN MUST NOTICE BE SENT?**

The notification must be made 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 and to restore the reasonable integrity of the data system. Mont. Code § 30-14-1704(1).

**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 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 electronic mail notice when the person or business has an electronic mail address for the subject persons; and

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

(3) notification to applicable local or statewide media. Mont. Code §§ 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 this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the data system. Mont. Code § 30-14-1704(6).

**WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?**

The statute does not specify who may enforce or what penalties may be imposed.

**ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?**

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 this part 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 of the security of the system if the personal information was or is reasonably believed to have been acquired by an unauthorized person.

Licensees, insurance-support organizations, and persons to whom personal information is disclosed pursuant to this part 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.

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 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 § 33-19-321.

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.

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:

(i) 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

(ii) 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).

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 notification of the breach in the manner required by subsection (2)(a) but shall provide notification if the third-party fails to do so in a reasonable time and may recover from the third-party its reasonable costs for providing the notice.

A state agency or third-party that is required to issue a notification to an individual pursuant to this section 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 person, a single copy of the notification that includes the number of people who were notified must be submitted to the Chief Information Officer and the Consumer Protection Office. Mont. Code § 2-6-1503.

## NEBRASKA

**STATUTE:** Neb. Rev. Stat. §§ **87-801**,[45] **802**,[46] **803**,[47] **804**,[48] **805**,[49] **806**,[50] **807**.[51]

### WHO MUST COMPLY?

An individual or a commercial entity that conducts business in Nebraska and that owns, maintains, or licenses computerized data that includes personal information about a resident of Nebraska. Neb. Rev. Stat. § 87-801.

### 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:

(A) social security number;

(B) motor vehicle operator's license number or state identification card number;

(C) 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;

(D) unique electronic identification number or routing code, in combination with any required security code, access code, or password;

(E) unique biometric data, such as a fingerprint, voice print, or retina or iris image, or other unique physical representation; or

(F) a user name or email 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.

### 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. Good faith acquisition of personal information by an employee or agent of an individual

[45] *Available at*: **http://nebraskalegislature.gov/laws/statutes.php?statute=87-801**.
[46] *Available at*: **http://nebraskalegislature.gov/laws/statutes.php?statute=87-802**.
[47] *Available at*: **http://nebraskalegislature.gov/laws/statutes.php?statute=87-803**.
[48] *Available at*: **http://nebraskalegislature.gov/laws/statutes.php?statute=87-804**.
[49] *Available at*: **http://nebraskalegislature.gov/laws/statutes.php?statute=87-805**.
[50] *Available at*: **http://nebraskalegislature.gov/laws/statutes.php?statute=87-806**.
[51] *Available at*: **http://nebraskalegislature.gov/laws/statutes.php?statute=87-807**.

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(4).

The statute does not apply if the data subject to the breach is encrypted. Encrypted means converted by 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. 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 the Attorney General.

If the breach affects a person that maintains or stores covered information, that person must notify the owner or licensee of that information. Neb. Rev. Stat. § 87-803(3).

**WHEN MUST NOTICE BE SENT?**

Notice shall 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).

**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 that the cost of providing notice will exceed 75,000, that the affected class of Nebraska residents to be notified exceeds 100,000 residents, or that the individual or commercial entity does not have sufficient contact information to provide notice.

Substitute notice under this subdivision requires all of the following:

(i) electronic mail notice if the individual or commercial entity has electronic mail addresses for the members of the affected class of Nebraska residents;

(ii) 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

(iii) notice to major statewide media outlets.

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 under this subdivision requires all of the following:

(i) electronic mail notice if the individual or commercial entity has electronic mail addresses for the members of the affected class of Nebraska residents;

(ii) 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;

(iii) 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

(iv) notification to major media outlets in the geographic area in which the individual or commercial entity is located. Neb. Rev. Stat. § 87-802(4).

**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.

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.

**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.

The statute does not address a private right of action.

**ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?**

None.

## NEVADA

**STATUTE:** Nev. Rev. Stat. §§ **603A.010 *et seq.***,[52] **242.183**.[53]

### WHO MUST COMPLY?

Any data collector that owns, maintains, or licenses computerized data which includes personal information must disclose a breach to affected residents of the State. "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.

The following data is not covered: (1) the last four digits of a social security number, (2) the last four digits of a driver's license number, (3) the last four digits of a driver authorization card number, (4) the last four digits of an identification card number, or (5) publicly available information that is lawfully made available to the general public from federal, state or local governmental records. Nev. Rev. Stat. § 603A.040.

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

[52] *Available at*: **http://www.leg.state.nv.us/NRS/NRS-603A.html**.
[53] *Available at*: **http://www.leg.state.nv.us/NRS/NRS-242.html#NRS242Sec183**.

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.

**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. If the breach affects a person that maintains or stores covered information, that person must notify the owner or licensee of that information. Nev. Rev. Stat. § 603A.220.

If a data collector determines that notification is required to be given pursuant to the provisions of this section to more than 1,000 persons at any one time, the data collector shall also notify, without unreasonable delay, any consumer reporting agency, as that term is defined in 15 U.S.C. § 1681a(p), 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.

**WHEN MUST NOTICE BE SENT?**

Disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system data. Nev. Rev. Stat. § 603A.220.

**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;

(2) 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

(3) Substitute notification, if the data collector demonstrates that the cost of providing notification would exceed $250,000, the affected class of subject persons to be notified exceeds 500,000, or the data collector does not have sufficient contact information. Nev. Rev. Stat. § 603A.220.

Substitute notification must consist of all the following:

(i) notification by electronic mail when the data collector has electronic mail addresses for the subject persons;

(ii) conspicuous posting of the notification on the Internet website of the data collector, if the data collector maintains an Internet website; and

(iii) notification to major statewide media. Nev. Rev. Stat. § 603A.220.

**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 this section:

(1) maintains its own notification policies and procedures as part of an information security policy for the treatment of personal information that is otherwise consistent with the timing requirements of this section if the data collector notifies subject persons in accordance with its policies and procedures in the event of a breach of the security of the system data; or

(2) is subject to and complies with the privacy and security provisions of the Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801 *et seq.* Nev. Rev. Stat. § 603A.220.

**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 this chapter, the Attorney General or district attorney may bring an action against that person to obtain a temporary or permanent injunction against the violation. Nev. Rev. Stat. § 603A.920.

In addition to any other penalty provided by law for the breach of the security of the system data maintained by a data collector, the court may order a person who is convicted of unlawfully obtaining or benefiting from personal information obtained as a result of such breach to pay restitution to the data collector for the reasonable costs incurred by the data collector in providing the notification required pursuant to § 603A.220, including, without limitation, labor, materials, postage and any other costs reasonably related to providing such notification. Nev. Rev. Stat. § 603A.910.

A data collector that provides the notification required pursuant to § 603A.220 may commence an action for damages against a person that unlawfully obtained or benefited from personal information obtained from records maintained by the data collector. A data collector that prevails in such an action may be awarded damages which may include, without limitation, the reasonable costs of notification, reasonable attorney's fees and costs and punitive damages when appropriate. The costs of notification include, without limitation, labor, materials, postage and any other costs reasonably related to providing the notification. Nev. Rev. Stat. § 603A.900.

**ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?**

The Chief of the Office of Information Security shall investigate and resolve any breach of an information system of a State agency or elected officer that uses the equipment or services of the Division or an application of such an information system or unauthorized acquisition of

computerized data that materially compromises the security, confidentiality or integrity of such an information system.

The Administrator or Chief of the Office of Information Security, at his or her discretion, may inform members of the Technological Crime Advisory Board created by § 205A.040, the Nevada Commission on Homeland Security created by § 239C.120 and the Information Technology Advisory Board created by § 242.122 of any breach of an information system of a State agency or elected officer or application of such an information system or unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of such an information system. Nev. Rev. Stat. § 242.183.

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 shall 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. §§ **359-C:19**,[54] **C:20**,[55] **C:21**;[56] **189:66**.[57]

### WHO MUST COMPLY?

Any person doing business in the State who owns, maintains, or licenses computerized data that includes personal information. N.H. Rev. Stat. § 359-C:20.

### WHAT DATA IS COVERED?

Personal information, which is 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.

### 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.

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 for purposes of this subdivision 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.

---

[54] *Available at*: **http://www.gencourt.state.nh.us/rsa/html/XXXI/359-C/359-C-19.htm**.
[55] *Available at*: **http://www.gencourt.state.nh.us/rsa/html/XXXI/359-C/359-C-20.htm**.
[56] *Available at*: **http://www.gencourt.state.nh.us/rsa/html/XXXI/359-C/359-C-21.htm**.
[57] *Available at*: **http://www.gencourt.state.nh.us/rsa/html/XV/189/189-66.htm**.

**WHO MUST BE NOTIFIED?**

Any affected individuals. Any person engaged in trade or commerce that is subject to § 358-A:3 shall also notify the regulator which has primary regulatory authority over such trade or commerce. All other persons shall notify the New Hampshire Attorney General's Office.

If the breach affects a person that maintains or stores covered information, that person must notify the owner or licensee of that information.

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, as defined by 15 U.S.C. § 1681a(p), 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. Nothing in this paragraph shall be construed to require the person to provide to any consumer reporting agency the names of the consumers entitled to receive the notice or any personal information relating to them. N.H. Rev. Stat. § 359-C:20(VI).

**WHEN MUST NOTICE BE SENT?**

Notification must be sent immediately following discovery, unless a delay is required by law enforcement, or a national or homeland security agency. N.H. Rev. Stat. § 359-C:20(II).

**IN WHAT FORM AND MANNER MUST NOTICE BE SENT?**

The notice required under this section shall 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 person or business who notifies affected persons;

(4) substitute notice, if the person demonstrates that the cost of providing notice would exceed $5,000, that the affected class of subject individuals to be notified exceeds 1,000, or that the person does not have sufficient contact information or consent to provide notice pursuant to subparagraphs I(a)-I(c); 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. N.H. Rev. Stat. § 359-C:20(III).

Substitute notice shall consist of all of the following:

(i) email notice when the person has an email address for the affected individuals;

(ii) conspicuous posting of the notice on the person's business website, if the person maintains one; and

(iii) notification to major statewide media.

**WHAT MUST THE NOTICE SAY?**

Notice under this section shall 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 person subject to this section. N.H. Rev. Stat. § 359-C:20(IV).

Notice sent to a regulatory authority shall include the anticipated date of the notice to the individuals and the approximate number of individuals in this state who will be notified. Nothing in this section shall be construed to require the person to provide to any regulator or the New Hampshire attorney general's office 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).

**ARE THERE ANY EXEMPTIONS?**

Any person engaged in trade or commerce that is subject to § 358-A:3 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 with this subdivision 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 New Hampshire Attorney General's Office shall enforce the provisions of this subdivision pursuant to § 358-A:4. The burden shall be on the person responsible for the determination under § 359-C:20 to demonstrate compliance with this subdivision. N.H. Rev. Stat. § 359-C:21.

Whenever the Attorney General has reason to believe that trade or commerce declared unlawful by this chapter has been, is being or is about to be conducted by, any person, the Attorney General may bring an action in the name of the State against such person to restrain by temporary or permanent injunction the use of such trade or commerce and may petition the court for an order of restitution of money or property to any person or class of persons injured thereby. The action may be brought in the Superior Court of the County in which the person allegedly in violation of this chapter resides or in which the principal place of business is located, or, with the consent of the parties or if the person is a nonresident and has no place of business within the State, in the Superior Court of Merrimack County. N.H. Rev. Stat. § 358-A:4.

Upon a finding that any person has engaged or is engaging in any act or practice declared unlawful by this chapter, the court may make any necessary order or judgment and may award to the State civil penalties up to $10,000 for each violation of this chapter. No such order shall require the payment of civil penalties until the process of appeal has been exhausted. Any such order or judgment shall be prima facie evidence in any action brought under § 358-A:10 that the respondent has engaged in an act or practice declared unlawful by this chapter. For the purpose of this section, the court shall determine the number of unlawful acts or practices which have occurred without regard to the number of persons affected thereby. It shall be an affirmative defense to the assessment of civil penalties that the defendant acted pursuant to a good faith misunderstanding concerning the requirements of this chapter. N.H. Rev. Stat. § 358-A:4.

Any person injured by any violation under this subdivision may bring an action for damages and for such equitable relief, including an injunction, as the court deems necessary and proper. If the court finds for the plaintiff, recovery shall be in the amount of actual damages. If the court finds that the act or practice was a willful or knowing violation of this chapter, it shall award as much as 3 times, but not less than 2 times, such amount. In addition, a prevailing plaintiff shall be awarded the costs of the suit and reasonable attorney's fees, as determined by the court. Any attempted waiver of the right to the damages set forth in this paragraph shall be void and unenforceable. Injunctive relief shall be available to private individuals under this chapter without bond, subject to the discretion of the court. N.H. Rev. Stat. § 359-C:21.

**ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?**

Section 189:66 requires schools to create a security plan which includes notification requirements. The security plan shall:

(1) require notification as soon as practicable to:

(i) 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; and

(ii) 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 § 193-C:7, and Commissioner of the Department of Information Technology; and

(2) require the Department 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 § 193-C:7, and Commissioner of the Department of Information Technology. The breach report shall also be posted to the Department's public Internet website and shall not include any information that itself would pose a security threat to a database or data system. The report shall include:

(i) the name of the organization reporting the breach;

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

(iii) the date, estimated date, or date range of the breach;

(iv) a general description of the breach incident;

(v) the estimated number of students and teachers affected by the breach, if any; and

(vi) information about what the reporting organization has done to protect individuals whose information has been breached. N.H. Rev. Stat. § 189:66.

## NEW JERSEY

**STATUTE:** N.J. Stat. §§ **56:8-161, 163**.[58]

### WHO MUST COMPLY?

Any business that conducts business in New Jersey, or any public entity that compiles or maintains computerized records that include personal information of residents of the State, even if done on behalf of another business or public entity. 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; 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.

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

The statute does not apply if the data subject to the breach is encrypted or has been secured by any other method or technology that renders the personal information unreadable or unusable. The statute does not define encryption.

### WHO MUST BE NOTIFIED?

Any customer who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person. N.J. Stat. § 56:8-161(a).

If the breach affects a person that maintains or stores covered information, that person must notify the owner or licensee of that information, who shall notify its New Jersey customers. N.J. Stat. § 56:8-163(b).

---

[58] *Available at*: **http://lis.njleg.state.nj.us/cgi-bin/om_isapi.dll?clientID=33831296&depth=2&expandheadings=off&headingswithhits=on&infobase=statutes.nfo&softpage=TOC_Frame_Pg42**.

The Division of State Police in the Department of Law and Public Safety must also be notified before the business or public entity discloses the breach to the costumer. N.J. Stat. § 56:8-163(c).

In the event that a business or public entity discovers circumstances requiring notification pursuant to this section of more than 1,000 persons at one time, the business or public entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile or maintain files on consumers on a nationwide basis, as defined by subsection (p) of section 603 of the federal Fair Credit Reporting Act (15 U.S.C. § 1681a), of the timing, distribution and content of the notices. N.J. Stat. § 56:8-163(f).

Disclosure of a breach of security to a customer shall not be required under the statute 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 five years. N.J. Stat. § 56:8-163(a).

**WHEN MUST NOTICE BE SENT?**

The disclosure to a customer shall 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).

**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 (15 U.S.C. § 7001); or

(3) substitute notice, if the business or public entity 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 business or public entity does not have sufficient contact information.

Substitute notice shall consist of all of the following:

(i) email notice when the business or public entity has an email address;

(ii) conspicuous posting of the notice on the Internet web site page of the business or public entity, if the business or public entity maintains one; and

(iii) notification to major statewide media. N.J. Stat. § 56:8-163(d).

**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 be in compliance 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?**

The statute does not address who may enforce.

**ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?**

None.

## NEW MEXICO

**STATUTE:** None. Pending legislation: **H.B. 325**.[59]

H.B. 325 *Status*: Action Postponed Indefinitely. Relates to consumer protection; creates the data breach notification act; requires notification to persons affected by a security breach involving personal identifying information; requires secure storage and disposal of data containing personal identifying information; requires notification to consumer reporting agencies, the office of the attorney general and card processors in certain circumstances; provides civil penalties.

[59] https://www.nmlegis.gov/Legislation/Legislation?Chamber=H&LegType=B&LegNo=%20325&year=16.

## NEW YORK

**STATUTE:** N.Y. Gen. Bus. Law § **899-aa**,[60] N.Y. State Tech. Law § **208**.[61]

### WHO MUST COMPLY?

Any person or business which conducts business in New York State, and which owns, licenses, or maintains computerized data which includes private information. Any person or business which maintains computerized data which includes private information that such person or business does not own. N.Y. Gen. Bus. Law §§ 899-aa(2), (3).

### 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.

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).

The statute does not apply if the data subject to the breach is encrypted. The statute does not define encryption. N.Y. Gen. Bus. Law § 899-aa(1)(b). This exception does not apply if the encryption is compromised.

### WHAT CONSTITUTES A DATA BREACH?

The unauthorized acquisition 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(3)(c).

### WHO MUST BE NOTIFIED?

If the breach affects a person that maintains or stores covered information, that person must notify the owner or licensee of that information. N.Y. Gen. Bus. Law § 899-aa(3).

---

[60] *Available at*: **http://public.leginfo.state.ny.us/navigate.cgi**.
[61] *Available at*: **http://public.leginfo.state.ny.us/navigate.cgi**.

Affected persons must be notified, as well as the State Attorney General, the Department of State and the Division of State Police as to the timing, and distribution of the notices and approximate number of affected persons.

In the event that more than 5,000 New York residents are to be notified at one time, the person or business shall also notify consumer reporting agencies as to the timing, content and distribution the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York residents. N.Y. Gen. Bus. Law §§ 899-aa(8)(a), (b).

**WHEN MUST NOTICE BE SENT?**

Notice must be sent immediately following discovery, consistent with law enforcement needs. N.Y. Gen. Bus. Law §§ 899-aa(1), (3).

**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 said notice in electronic form and a log of each such notification is kept by the person or business who notifies affected persons in such form; provided further, however, that in no case shall any person or business require a person to consent to accepting notice in such form as a condition of establishing any business relationship or engaging in any transaction;

(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 5,000, or such business does not have sufficient contact information.

Substitute notice shall consist of all of the following: (1) email notice when such business has an email address for the subject persons; (2) conspicuous posting of the notice on such business' web site page, 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?**

Such notice shall include contact information for the person or business making the notification and a description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so 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 Attorney General may enforce the statute. In such action, preliminary relief may be granted under article sixty-three of the civil practice law and rules. In such action the court may award damages for actual costs or losses incurred by a person entitled to notice pursuant to this article, if notification was not provided to such person pursuant to this article, including consequential financial losses. Whenever the court shall determine in such action that a person or business violated this article knowingly or recklessly, the court may impose a civil penalty of the greater of $5,000 or up to $10 per instance of failed notification, provided that the latter amount shall not exceed $150,000. N.Y. Gen. Bus. Law § 899-aa(6)(a).

The Attorney General may seek injunctive relief and damages for actual costs or losses incurred as a result of the breach. The Attorney General may also seek a statutory penalty of up to $150,000 if the defendant knowingly or recklessly violated the statute. N.Y. Gen. Bus. Law § 899-aa(6)(a).

There is no private right of action.

New York City Administrative Code § 20-117 contains a notice statute with the same requirements in the event of a data breach. Sub-section (h) allows for a fine of up to $500 for a person that violates the statute, as well as a civil penalty of $100 for each violation.

## ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

None.

## NORTH CAROLINA

**STATUTE:** N.C. Gen. Stat. §§ **75-61**,[62] **75-65**.[63]

### WHO MUST COMPLY?

Any business that owns, licenses, or maintains personal information of residents of North Carolina or any business that conducts business in North Carolina that owns, licenses, or maintains 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. 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.

(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 as defined in § 14-113.8(6);

(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;

(11) biometric data;

(12) fingerprints;

---

[62] *Available at*: **http://www.ncga.state.nc.us/EnactedLegislation/Statutes/HTML/BySection/Chapter_75/GS_75-61.html**.
[63] *Available at*: **http://www.ncga.state.nc.us/EnactedLegislation/Statutes/HTML/BySection/Chapter_75/GS_75-65.html**.

(13) passwords; or

(14) parent's legal surname prior to marriage. N.C. Gen. Stat. § 75-61-10.

**WHAT CONSTITUTES A DATA BREACH?**

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

Good faith acquisition of personal information by an employee or agent of the business for a legitimate purpose is not a security breach, provided that the personal information is not used for a purpose other than a lawful purpose of the business and is not subject to further unauthorized disclosure. N.C. Gen. Stat. § 75-61-1.

If accessed data is encrypted, the statute does not apply. 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.

**WHO MUST BE NOTIFIED?**

The business must notify the affected person and provide the Consumer Protection Division of the 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.

In the event a business provides notice to more than 1,000 persons at one time pursuant to this section, the business shall notify, without unreasonable delay, the Consumer Protection Division of the Attorney General's Office 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), of the timing, distribution, and content of the notice.

If the breach affects a person that maintains or stores covered information, that person must notify the owner or licensee of that information. N.C. Gen. Stat. § 75-61(b).

**WHEN MUST NOTICE BE SENT?**

The disclosure notification shall 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).

**IN WHAT FORM AND MANNER MUST NOTICE BE SENT?**

Notice to affected persons must be provided by one of the following methods:

(1) written notice;

(2) electronic notice, for those persons for whom it 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;

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

(4) substitute notice, 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, or if the business does not have sufficient contact information or consent to satisfy subdivisions (1), (2), or (3) of this subsection, for only those affected persons without sufficient contact information or consent, or 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 shall consist of all the following: (a) email notice when the business has an electronic mail address for the subject persons; (b) conspicuous posting of the notice on the Web site page of the business, if one is maintained; and (c) notification to major statewide media. N.C. Gen. Stat. § 75-65(e).

**WHAT MUST THE NOTICE SAY?**

The notice shall be clear and conspicuous. The notice shall 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. § 75-61-10(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.

## WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

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

## ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

None.

## NORTH DAKOTA

**STATUTE:** N.D. Cent. Code §§ **51-30-01** ***et seq.***,[64] **51-59-34(4)(d)**.[65]

### WHO MUST COMPLY?

Any person that owns, maintains or licenses computerized data that includes personal information of a resident of the State. 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 § 39-06-14;

(3) a non-driver color photo identification card number assigned to the individual by the Department of Transportation under § 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) medical information;

(8) health insurance information;

(9) an identification number assigned to the individual by the individual's employer in combination with any required security code, access code, or password; or

(10) the individual's digitized or other electronic signature. N.D. Cent. Code § 51-30-02(4).

The statute does not apply if the data subject to the breach are secured by encryption or by any other method or technology that renders the electronic files, media, or databases unreadable or unusable. N.D. Cent. Code § 51-30-01(1).

### WHAT CONSTITUTES A DATA BREACH?

The unauthorized acquisition of computerized data when access to personal information has not

[64] *Available at*: **http://www.legis.nd.gov/cencode/t51c30.pdf**.
[65] *Available at*: **http://www.legis.nd.gov/cencode/t54c59.pdf?20151022172303**.

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 the State whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. In addition, any person that experiences a breach of the security system as provided in the statute shall disclose to the Attorney General by mail or email any breach of the security system which exceeds 250 individuals. N.D. Cent. Code § 51-30-02.

If the breach affects a person that maintains or stores covered information, that person must notify the owner or licensee of that information. N.D. Cent. Code § 51-30-03.

**WHEN MUST NOTICE BE SENT?**

The disclosure must be made immediately following discovery, in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in § 51-30-04, or any measures necessary to determine the scope of the breach and to restore the integrity of the data system. N.D. Cent. Code § 51-30-03.

**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: (a) electronic mail notice when the person has an electronic mail address for the subject persons; (b) conspicuous posting of the notice on the person's website page, if the person maintains one; and (c) 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?

Notwithstanding § 51-30-05, a person that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this chapter is deemed to be in compliance with the notification requirements of this chapter if the person notifies subject individuals in accordance with its policies in the event of a breach of security of the system.

A financial institution, trust company, or credit union that is subject to, examined for, and in compliance with the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice is in compliance with this chapter.

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 this chapter. N.D. Cent. Code § 51-30-06.

## WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?

The Attorney General may enforce this chapter. The Attorney General, in enforcing this chapter, has all the powers provided in chapter 51-15 and may seek all the remedies in chapter 51-15. A violation of this chapter is deemed a violation of chapter 51-15. The remedies, duties, prohibitions, and penalties of this chapter are not exclusive and are in addition to all other causes of action, remedies, and penalties under chapter 51-15, or otherwise provided by law. N.D. Cent. Code § 51-30-07.

N.D. Cent. Code § 51-15-11 allows courts to impose a civil penalty of not more than $5,000 for each violation of this chapter or for each violation of chapter 51-12, 51-13, 51-14, or 51-18.

N.D. Cent. Code § 51-15-11 allows the Attorney General to seek an injunction, an order appointing a receiver, cease and desist order, or civil penalties.

## ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

None.

## OHIO

**STATUTE:** Ohio Rev. Code §§ **1347.12**,[66] **1349.19**,[67] **1349.191**,[68] **1349.192**.[69]

### WHO MUST COMPLY?

Ohio governmental agencies, individuals, and entities that conduct business in Ohio and own, license, or maintain computerized data that includes personal information about Ohio residents.

Ohio Rev. Code § 1347.12 governs agency disclosure of security breach of computerized personal information data. (State agencies or agencies of a political subdivision). Ohio Rev. Code § 1349.19(C).

Ohio Rev. Code § 1349.19 governs private disclosure of security breach of computerized personal information data. (Any person that owns or licenses computerized data that includes personal information). Ohio Rev. Code § 1349.19(B)(1).

### WHAT DATA IS COVERED?

"Personal information" means an individual's first name or first initial and last name, in combination with one of the following data elements:

- a social security number;
- a driver's license number or state identification card number; or
- an account number or credit/debit card number in combination with any required access code to that account or card.

"Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. Ohio Rev. Code § 1349.19(A)(7).

The notification requirements are not triggered if these data elements are encrypted, redacted to four digits, or otherwise made to be unreadable. "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

[66] *Available at*: **http://codes.ohio.gov/orc/1347.12**.
[67] *Available at*: **http://codes.ohio.gov/orc/1349.19**.
[68] *Available at*: **http://codes.ohio.gov/orc/1349.191**.
[69] *Available at*: **http://codes.ohio.gov/orc/1349.192**.

or confidentiality of personal information owned or licensed by a person, state agency or an agency of a political subdivision 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.

**WHO MUST BE NOTIFIED?**

Any resident of the State whose personal information was, or reasonably is believed to have been, accessed. Ohio Rev. Code § 1349.19(B)(1).

If circumstances require disclosure to more than 1,000 residents of the State involved in a single occurrence of a breach of the security of the system, the person shall 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 the residents of the State. In no case shall a person that is required to make a notification delay any disclosure or notification in order to make the notification required by this division.

Third-parties that maintain computerized data must notify the owners or licensors of that data. Ohio Rev. Code § 1349.19(C).

**WHEN MUST NOTICE BE SENT?**

In the most expedient time possible, but not later than 45 days following its discovery or notification of the breach in the security of the system, subject to the legitimate needs of law enforcement activities.

Notification from a third-party that maintains computerized personal information on behalf of another person must be sent to that person as expeditiously as possible. Ohio Rev. Code § 1349.19(C).

**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 disclose demonstrates that the person does not have sufficient contact information to provide notice using the above methods, or that the cost of providing disclosure or notice to residents to whom disclosure or notification is

> required would exceed $250,000, or that the affected class of subject residents to whom disclosure or notification is required exceeds 500,000 persons. Ohio Rev. Code § 1349.19(E).

Substitute notice is permitted if the person required to disclose demonstrates that it is a business entity with 10 or less employees and that the cost of providing the disclosures or notices to residents to whom disclosure or notification is required will exceed $10,000. Ohio Rev. Code § 1349.19(E).

The disclosure may be made pursuant to any provision of a contract entered into by the person with another person prior to the date that the breach of the security of the system occurred if that contract does not conflict with any provision of this section and does not waive any provision of this section. Ohio Rev. Code § 1349.19(E).

**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 of a financial institution, trust company, or credit union that is required by federal law, including, but not limited to, any federal statute, regulation, regulatory guidance, or other regulatory action, to notify its customers of an information security breach with respect to information about those customers and that is subject to examination by its functional government regulatory agency for compliance with the applicable federal law, is exempt from the requirements of this section. Ohio Rev. Code § 1349.19(F)(1).

In addition, the statute does not apply to covered entities under HIPAA. Ohio Rev. Code § 1349.19(F)(2).

**WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?**

The Attorney General may conduct an investigation and bring a civil action upon an alleged failure by a person to comply with the requirements of the statute. Ohio Rev. Code § 1349.19(I). No other penalty is specified in the statute.

**ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?**

Under an Ohio Department of Insurance (ODI) bulletin that became effective November 2, 2009, all persons or entities holding a license or certificate of authority from the Superintendent of Insurance are required to notify ODI within 15 calendar days of discovering a "loss of control" of policyholders' personal information. The notification to ODI is required for incidents affecting more than 250 Ohio residents. "Loss of control" is defined as the unauthorized access to, unauthorized acquisition of, or disappearance of any Personal Information, including with respect to computerized data the unauthorized access to and/or acquisition of that computerized data that compromises the security or confidentiality of Personal Information" The definition of personal information is the common definition used in most state data breach laws—the

individual's first name or first initial and last name in combination with a social security number, driver's license number, state identification number, or bank/credit/debit card or account number. Bulletin 2009-12.

## OKLAHOMA

**STATUTE:** Okla. Stat. §§ **74-3113.1, 24-161-166**.[70]

**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. § 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.

The statute does not apply if affected data is encrypted or redacted. "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)(c).

**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

[70] *Available at*: http://www.oklegislature.gov/osstatuestitle.html.

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. Okl. 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 covered data held by a person on behalf of another covered entity, notice must be sent as soon as practicable following discovery. Okl. Stat. § 24-163.

**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. Okl. Stat. Ann. § 24-162(7).

Substitute notice consists of any two of the following:

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

(ii) 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;

(iii) notice to major statewide media. Okl. Stat. Ann. § 24-162(7).

**WHAT MUST THE NOTICE SAY?**

The statute does not specify the contents of the notification.

**ARE THERE ANY EXEMPTIONS?**

Yes:

(A) 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

(B) 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. Okl. 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. Ann. §§ 24-165.

**ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?**

None.

## OREGON

**STATUTE:** Or. Rev. Stat. §§ **646A.600-628**,[71] **2015 S.B. 601, Chap. 357**.[72]

### WHO MUST COMPLY?

A person that owns, licenses, or maintains 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. Rev. Stat. §§ 646a.604(1), (2)

### WHAT DATA IS COVERED?

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

(A) a consumer's social security number;

(B) a consumer's driver license number or state identification card number issued by the Department of Transportation;

(C) a consumer's passport number or other identification number issued by the United States;

(D) 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;

(E) 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;

(F) 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; or

(G) 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).

The statute does not apply if the data is encrypted unless the breach involves encrypted data and the encryption key has been compromised. "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).

---

[71] *Available at*: https://www.oregonlegislature.gov/Pages/PageNotFoundError.aspx?requestUrl=https://www.oregonlegislature.gov/bills_laws/lawsstatutes/2013ors646A.html.

[72] *Available at*: **https://www.oregonlegislature.gov/bills_laws/lawsstatutes/2015orLaw0357.pdf**.

## 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)

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, or under license 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, consistent with the legitimate needs of law enforcement, and consistent with any measures that are necessary to determine sufficient contact information for the affected consumer, determine the scope of the breach of security, and restore the reasonable integrity, security and confidentiality of the personal information. Or. Rev. Stat. § 646A.604(1).

## 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).

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(7).

**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 owned or licensed the personal information that was subject to the breach of security;

(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?**

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(8).

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(8)(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 INDUSTRY-SPECIFIC REQUIREMENTS?**

None.

## PENNSYLVANIA

**STATUTE:** 73 Pa. Stat. § **2301** ***et seq.***[73]

### WHO MUST COMPLY?

Any entity that maintains, stores or manages computerized data that includes personal information regarding a Pennsylvania resident. 73 P.S. § 2303(a), (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 P.S. § 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 P.S. § 2303.

### WHAT CONSTITUTES A DATA BREACH?

The unauthorized access or 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 P.S. § 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 P.S. § 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 P.S. § 2303(c).

If more than 1,000 persons are notified, all nationwide CRAs must be notified without unreasonable delay of timing. 73 P.S. § 2305.

### WHEN MUST NOTICE BE SENT?

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

[73] *Available at*: **https://govt.westlaw.com/pac/index?__lrTS=20160526195352426&transitionType=Default&contextData=(sc.Default)**.

writing that notification will impede a criminal or civil investigation. 73 P.S. § 2303(a).

**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:

(i) the cost of providing notice would exceed $100,000;

(ii) the affected class of subject persons to be notified exceeds 175,000; or

(iii) the entity does not have sufficient contact information.

Substitute notice shall consist of all of the following: (a) email notice when the entity has an email address for the subject persons; (b) conspicuous posting of the notice on the entity's Internet website if the entity maintains one; and (c) notification to major Statewide media. 73 P.S. § 2302.

**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 provide a telephone number or website for further information or assistance. 73 P.S. § 2302.

**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 P.S. § 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 P.S. § 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 P.S. § 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 P.S. § 2308. Private rights of action are not permitted. No other penalties are specified in the statute.

**ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?**

None.

## PUERTO RICO

**STATUTE:** 10 Laws of Puerto Rico § **4051** ***et seq.***[74]

### WHO MUST COMPLY?

Any entity that is the owner or custodian of a database that includes personal information of residents of Puerto Rico. "Entity" refers to every agency, board, body, examining board, corporation, public corporation, committee, independent office, division, administration, bureau, department, authority, official, instrumentality or administrative organism of the three branches of the Government; every corporation, partnership, association, private company or organization authorized to do business or operate in the Commonwealth of Puerto Rico; as well as every public or private educational institution, regardless of the level of education offered by it. § 4051(d).

### 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:

- social security number;
- driver license number, voter's identification or other official identification;
- bank or financial account numbers of any type with or without passwords or access code that may have been assigned;
- names of users and passwords or access codes to public or private information systems;
- medical information protected by the Health Insurance Portability and Accountability Act ("HIPAA");
- tax information; or
- work-related evaluations. 10 L.P.R.A. § 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 L.P.R.A. § 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

[74] *Available at*: **http://www.lexisnexis.com/hottopics/lawsofpuertorico/**.

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 physical access to the recording media that contain the same and any removal or undue retrieval of the recordings. 10 L.P.R.A. § 4051(c).

**WHO MUST BE NOTIFIED?**

Any citizen of Puerto Rico whose personal information has been subject to a security violation. 10 L.P.R.A. § 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 L.P.R.A. § 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 L.P.R.A. § 4052.

**IN WHAT FORM AND MANNER MUST NOTICE BE SENT?**

Notice must be provided by one of the following methods:

- written notice; or
- authenticated electronic means according to the Digital Signatures Act.

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:

- 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
- 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 L.P.R.A. § 4053.

**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 L.P.R.A. § 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 L.P.R.A. § 4055.

**ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?**

None.

## RHODE ISLAND

**STATUTE:** R.I. Gen. Laws § **11-49.3-1** ***et seq.***[75]

### WHO MUST COMPLY?

Any State agency or person that owns, maintains or licenses computerized data that includes personal information. R.I. Gen. Laws § 11-49.3-4(a)

### 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:

(A) social security number;

(B) driver's license number or Rhode Island Identification Card number; or

(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. R.I. Gen. Laws § 11-49.3-3(a).

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. R.I. Gen. Laws § 11-49.3-3(a).

### 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. R.I. Gen. Laws § 11-49.3-4(a)(1).

A breach, however, does not include good faith acquisition of the information.

### 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.

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. R.I. Gen. Laws § 11-49.3-

[75] *Available at*: http://webserver.rilin.state.ri.us/Statutes/title11/11-49.3/INDEX.HTM.

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. R.I. Gen. Laws § 11-49.3-4(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. R.I. Gen. Laws § 11-49.3-4(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.

**IN WHAT FORM AND MANNER MUST NOTICE BE SENT?**

Notice must be provided by one of the following methods:

(A) written notice;

(B) electronic notice; or

(C) 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. R.I. Gen. Laws § 11-49.3-3(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

(6) 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. R.I. Gen. Laws § 11-49.3-4(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. R.I. Gen. Laws § 11-49.3-5(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. R.I. Gen. Laws § 11-49.3-5(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. R.I. Gen. Laws § 11-49.3-5

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.

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.

**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. R.I. Gen. Laws § 11-49.2-3.

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. R.I. Gen. Laws § 11-49.3-2(a).

## SOUTH CAROLINA

**STATUTE:** S.C. Code § **39-1-90**,[76] **2013 H.B. 3248**.[77]

### 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).

### 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:

(A) social security number;

(B) driver's license number or state identification card number issued instead of a driver's license;

(C) 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

(D) 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.

Encrypted data is not subject to the statute. S.C. Code § 39-1-90(D)(1). The statute does not define encryption.

### 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).

### 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).

---

[76] *Available at*: **http://www.scstatehouse.gov/code/t39c001.php**.
[77] *Available at*: **http://www.scstatehouse.gov/sess120_2013-2014/bills/3248.htm**.

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).

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:

(A) written notice;

(B) electronic notice (consistent with the requirements of the statute);

(C) telephonic notice; or

(D) 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)

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 INDUSTRY-SPECIFIC REQUIREMENTS?**

None.

## SOUTH DAKOTA

**STATUTE:** No statute or pending legislation.

## TENNESSEE

**STATUTE:** Tenn. Code §§ **47-18-2107, 8-4-119**,[78] **2015 S.B. 416, Chap. 42**.[79]

### 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(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 data elements, when either the name or the data elements are not encrypted or otherwise publicly available:

(A) social security number;

(B) driver's license number; or

(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. Tenn. Code § 47–18–2107(a)(3)(A).

### 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 breach does not include the good faith acquisition of the information, as defined by the statute. In addition, the statute does not apply if the personal data that was lost, stolen or accessed by an unauthorized individual is encrypted. Tenn. Code § 47–18–2107(a)(3)(A).

### 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.

[78] *Available at*: **http://www.lexisnexis.com/hottopics/tncode/**.
[79] *Available at*: **http://www.tn.gov/sos/acts/109/pub/pc0042.pdf**.

**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).

**IN WHAT FORM AND MANNER MUST NOTICE BE SENT?**

Notice must be provided by one of the following methods:

(A) written notice;

(B) 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

(C) 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 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).

**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. The statute does not specify which State agency has enforcement authority, or the types of penalties, if any, may be imposed. **Back To TOC**

**ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?**

None.

## TEXAS

**STATUTE:** Tex. Bus. & Com. Code §§ **521.002, 521.053**;[80] Tex. Ed. Code § **37.007(b)(5)**;[81] Tex. Pen. Code § **33.02**.[82]

### 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:

(A) social security number;

(B) driver's license number or government issued identification number; or

(C) 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.

In addition, information that identifies an individual and relates to:

(A) the physical or mental health or condition of the individual;

(B) the provision of health care to the individual; or

(C) payment for the provision of health care to the individual. Tex. Bus. & Com. Code § 521.002(a)(2).

### 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. 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.

---

[80] *Available at*: http://www.statutes.legis.state.tx.us/Docs/BC/htm/BC.521.htm.
[81] *Available at*: http://www.statutes.legis.state.tx.us/Docs/ED/htm/ED.37.htm.
[82] *Available at*:
http://www.statutes.legis.state.tx.us/StatutesByDate.aspx?code=PE&level=SE&value=33.02&date=7/18/2015.

**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.

**WHEN MUST NOTICE BE SENT?**

Disclosure shall be made as quickly as possible, except if delay is requested by a law enforcement agency or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system. 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).

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:

(A) written notice to individual's last known address;

(B) electronic notice; or

(C) 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.

## 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. 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(g).

## ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?

None.

## UTAH

**STATUTE:** Utah Code §§ **13-44-101** ***et seq.***,[83] **53A-13-301**.[84]

### 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:

(i) social security number;

(ii) (A) 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

(iii) 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.

### 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.

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.

### WHO MUST BE NOTIFIED?

Any resident of Utah whose personal information has been affected. Utah Code § 13-44-202.

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

[83] *Available at*: **http://le.utah.gov/xcode/Title13/Chapter44/13-44.html?v=C13-44_1800010118000101**.
[84] *Available at*: **http://le.utah.gov/xcode/Title53A/Chapter13/53A-13-S301.html?v=C53A-13-S301_2015051220150512**.

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.

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:

(i) in writing by first-class mail to the most recent address the person has for the resident;

(ii) 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;

(iii) by telephone, including through the use of automatic dialing technology not prohibited by other law; or

(iv) 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).

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).

**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.

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.

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. Utah Code § 13-44-301.

**ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?**

None.

## VERMONT

**STATUTE:** Vt. Stat. Ann. tit. 9, §§ **2430, 2435**.[85]

**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.

"Data collector" may include the State, State agencies, political subdivisions of the State, public and private universities, privately and publicly held corporations, limited liability companies, financial institutions, retail operators, and any other entity that, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates, or otherwise deals with nonpublic personal information. Vt. Stat. Ann. tit. 9, § 2430.

**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 or protected by another method that renders them unreadable or unusable by unauthorized persons, and the information is not publicly available:

(A) social security number;

(B) motor vehicle operator's license number or non-driver identification card number;

(C) 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

(D) account passwords or personal identification numbers or other access codes for a financial account.

"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.

"Redaction" means the rendering of data so that it is unreadable or is 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.

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.

[85] *Available at*: **http://legislature.vermont.gov/statutes/chapter/09/062**.

Ann. tit. 9, § 2430.

**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 the data collector.

Factors to consider when determining if a breach has occurred include the following:

(A) indications that the information is in physical possession and control of unauthorized person;

(B) indications that the information has been downloaded or copied;

(C) indications that the information was used by unauthorized person; and

(D) indications that the information has been made public. Vt. Stat. Ann. tit. 9, § 2430(8).

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).

**WHO MUST BE NOTIFIED?**

Any resident of Vermont whose personal information has been affected. Vt. Stat. Ann. tit. 9, § 2435(b).

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(a)(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).

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:

(A) 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

(B) 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.

**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:

(A) direct notice, which may be by one of the following methods:

(i) written notice mailed to the consumer's residence;

(ii) 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

(iii) telephonic notice, provided that telephonic contact is made directly with each affected consumer and not through a prerecorded message; or

(B) Substitute notice, if: (i) the data collector demonstrates that the cost of providing written or telephonic notice to affected consumers would exceed $5,000.00; (ii) the class of affected consumers to be provided written or telephonic notice exceeds 5,000; or (iii) the data collector does not have sufficient contact information. Vt. Stat. Ann. tit. 9, § 2435.

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.

**WHAT MUST THE NOTICE SAY?**

Notice must be clear and conspicuous and include a description of: the incident in general terms (including the 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.

Notice to the government will include the date, discovery, and preliminary description of the security breach and the number of Vermont individuals affected.

**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 of a security breach is not required if the data collector establishes that misuse of personal information is not reasonably possible. Vt. Stat. Ann. tit. 9, § 2435.

**WHO MAY ENFORCE AND WHAT PENALTIES MAY BE IMPOSED?**

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. No penalties are specified in the statute. Vt. Stat. Ann. Tit. 9, § 2435(g).

**ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?**

On August 6, 2013, the Vermont Department of Financial Regulation issued Bulletin Number 3, which summarizes the amendments to the notice requirements in the Vermont Security Breach Notification Act, codified at Vt. Stat. Ann. tit. 9, §§ 2435(b) and (f) and effective May 13, 2013. The Bulletin provides that the 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**,[86] **32.1-127.1:05**,[87] **22.1-20.2**.[88]

### 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:

(A) social security number;

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

(C) 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.

### 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.

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(C).

"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).

---

[86] *Available at*: **http://law.lis.virginia.gov/vacode/18.2-186.6/**.
[87] *Available at*: **http://law.lis.virginia.gov/vacode/title32.1/chapter5/section32.1-127.1:05/**.
[88] *Available at*: **http://law.lis.virginia.gov/vacode/22.1-20.2/**.

**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:

(A) written notice to individual's last known address;

(B) telephone notice;

(C) electronic notice; or

(D) 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 (A)-(C).

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).

**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).

**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(J).

Virginia also allows a private right of action. Va. Code § 18.2-186.6(I)

**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.

## VIRGIN ISLANDS

**STATUTE:** V.I. Code tit. 14, § **2208**.[89]

### WHO MUST COMPLY?

Any agency that owns, maintains or licenses computerized data that includes personal information. 14 V.I.C. § 2208 (a).

### 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. 14 V.I.C. § 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. 14 V.I.C. § 2208(e).

The statute does not apply if the affected data is encrypted.

### 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. 14 V.I.C. § 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. 14 V.I.C. § 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. 14 V.I.C. § 2208(b).

[89] *Available at*: **http://www.lexisnexis.com/hottopics/vicode/**.

**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. 14 V.I.C. § 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. 14 V.I.C. § 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. 14 V.I.C. § 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:

(A) email notice when the agency has an email address for the subject persons;

(B) conspicuous posting of the notice on the agency's Web site page, if the agency maintains one; and

(C) notification to major territory-wide media. 14 V.I.C. § 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. 14 V.I.C. § 2208(h).

**WHO MAY ENFORCE?**

Not specified.

**ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?**

None.

## WASHINGTON

**STATUTE:** Wash. Rev. Code §§ **19.255.010**,[90] **42.56.590**,[91] **2015 H.B. 1078**.[92]

### 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).

### 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:

(A) social security number;

(B) driver's license number or Washington identification card number; or

(C) 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(5).

### 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 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

[90] *Available at*: **http://apps.leg.wa.gov/RCW/default.aspx?cite=19.255.010**.
[91] *Available at*: **http://apps.leg.wa.gov/RCW/default.aspx?cite=42.56.590**.
[92] *Available at*: http://app.leg.wa.gov/BillInfo/summary.aspx?bill=1078&year=2015.

subject consumers to a risk of harm. Wash. Rev. Code § 19.255.010(4).

**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.

**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(3).

**IN WHAT FORM AND MANNER MUST NOTICE BE SENT?**

Notice must be provided by one of the following methods:

(A) written notice;

(B) electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures; or

(C) 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.

**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").

**WHO MAY ENFORCE?**

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 seek treble damages under Washington's Unfair Business Practices law for a violation of the statute. Wash. Stat. § 19.86.090.

**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 two 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.V. Code § **46A-2A-101** ***et seq.***[93]

### WHO MUST COMPLY?

Individuals or entities that own, license, or maintain computerized data that includes personal information regarding a resident of West Virginia. W.V. 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:

(A) social security number;

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

(C) 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.V. 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.V. 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.V. Code § 46A-2A-101(1).

Breach does not include the good faith acquisition of the information, as defined by the statute. W.V. Code § 46A-2A-101(1).

### 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.V. Code § 46A-2A-102(a).

[93] *Available at*: **http://www.legis.state.wv.us/WVCODE/Code.cfm?chap=46a&art=2A%20-%202A**.

Consumer reporting agencies must be notified by the entity in cases where the notice must be provided to over 1,000 people. W.V. Code § 46A-2A-102(f).

An individual or entity that maintains covered data must notify the owner or licensee of that data. W.V. 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.V. 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).

Substitute notice consists of any two of the following:

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

(B) conspicuous posting of the notice on the website of the individual or the entity if the individual or the entity maintains a website; or

(C) notice to major statewide media. W.V. Code § 46A-2A-101(7).

**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.V. 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.V. Code § 46A-2A-103.

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.V. Code § 46A-2A-103.

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.V. Code § 46A-2A-103.

**WHO MAY ENFORCE?**

The Attorney General may enforce. Willful and repeated violations may result in penalties up to $150,000. W.V. Code § 46A-2A-104.

Violations by licensed financial institutions are enforced by their primary regulator. W.V. Code § 46A-2A-104(c).

**ARE THERE ANY INDUSTRY-SPECIFIC REQUIREMENTS?**

None.

## WISCONSIN

**STATUTE:** Wis. Stat. § **134.98**.[94]

**WHO MUST COMPLY?**

Any entity (a person other than an individual), which does any of the following:

(A) conducts business in the State and maintains personal information in the ordinary course of business;

(B) licenses personal information in the State;

(C) maintains for a resident of the State a depository account; or

(D) lends money to a resident of the State.

Entity includes all of the following:

(A) 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

(B) a city, village, town, or county. Wis. Stat. § 134.98(1).

**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:

(A) social security number;

(B) driver's license number or state identification number;

(C) 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;

(D) DNA profile; or

(E) 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).

"Publicly available information" is not covered and means any information that an entity

[94] *Available at*: http://docs.legis.wisconsin.gov/statutes/statutes/134/98.

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).

**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. Ann. § 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.

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:

(A) the breach does not create a material risk of identity theft or fraud to the subject of the personal information; or

(B) 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).

**WHAT MUST THE NOTICE SAY?**

The statute does not specify the contents of the notification.

**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.

**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.***[95]

**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. § 40-12-501(g).

**WHAT DATA IS COVERED?**

The first name or first initial and last name of a person in combination with one or more of the following data elements when either the name or the data elements are not redacted:

(A) social security number;

(B) driver's license number or Wyoming identification card number;

(C) 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;

(D) tribal identification card;

(E) federal or state government issued identification card;

(F) shared secrets or security tokens that are known to be used for data based authentication;

(G) a username or email address, in combination with a password or security question and answer that would permit access to an online account;

(H) a birth or marriage certificate;

(I) medical information;

(J) health insurance information; or

(K) unique biometric data. Wyo. Stat. § 40-12-501(a)(vii).

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).

[95] *Available at*: **http://legisweb.state.wy.us/NXT/gateway.dll?f=templates&fn=default.htm&vid**=.

## 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.

## 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:

(A) written notice;

(B) electronic mail notice; or

(C) substitute notice.

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.

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).

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. 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).

**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 INDUSTRY-SPECIFIC REQUIREMENTS?**

None.