

# COMPLYING WITH U.S. STATE AND TERRITORIAL SECURITY BREACH NOTIFICATION LAWS

Excerpted from Chapter 27 (Cybersecurity: Information, Network and Data Security) of  
*E-Commerce and Internet Law: Legal Treatise with Forms 2d Edition*  
A 5-volume legal treatise by Ian C. Ballon (Thomson/West Publishing, [www.IanBallon.net](http://www.IanBallon.net))

DAILY JOURNAL CYBERFORUM 2019  
LOS ANGELES  
FEBRUARY 26, 2019

**Ian C. Ballon**  
**Greenberg Traurig, LLP**

|                                                                                                                                                                            |                                                                                                                                                                                 |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Los Angeles:</b><br><b>1840 Century Park East, Ste. 1900</b><br><b>Los Angeles, CA 90067</b><br><b>Direct Dial: (310) 586-6575</b><br><b>Direct Fax: (310) 586-0575</b> | <b>Silicon Valley:</b><br><b>1900 University Avenue, 5th Fl.</b><br><b>East Palo Alto, CA 914303</b><br><b>Direct Dial: (650) 289-7881</b><br><b>Direct Fax: (650) 462-7881</b> |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

[Ballon@gtlaw.com](mailto:Ballon@gtlaw.com)  
<[www.ianballon.net](http://www.ianballon.net)>  
**LinkedIn, Twitter, Facebook: IanBallon**

This paper has been excerpted from *E-Commerce and Internet Law: Treatise with Forms 2d Edition*  
(Thomson West, [www.IanBallon.net](http://www.IanBallon.net)), the 5-volume legal treatise by Ian C. Ballon



## Ian C. Ballon

Shareholder

Internet, Intellectual Property & Technology Litigation

Admitted: California, District of Columbia and Maryland  
Second, Third, Fourth, Fifth, Seventh, Ninth, Eleventh and Federal  
Circuits

U.S. Supreme Court

JD, LL.M., CIPP

Ballon@gtlaw.com

LinkedIn, Twitter, Facebook

## Los Angeles

1840 Century Park East

Los Angeles, CA 90067

T 310.586.6575

F 310.586.0575

## Silicon Valley

1900 University Avenue

5th Floor

East Palo Alto, CA 94303

T 650.289.7881

F 650.462.7881

Ian Ballon is Co-Chair of Greenberg Traurig LLP's Global Intellectual Property & Technology Practice and represents Internet, mobile, entertainment and technology companies in defending data privacy, security breach and TCPA class action suits and in other intellectual property and technology litigation. A list of recent cases may be found at <http://www.gtlaw.com/ian-C-Ballon-Experience>.

He is also the author of the leading treatise on Internet law, *E-Commerce and Internet Law: Treatise with Forms 2d edition*, the 5-volume set published by West ([www.IanBallon.net](http://www.IanBallon.net)), which includes extensive coverage of security breach and data privacy issues. In addition, he is the author of *The Complete CAN-SPAM Act Handbook* (West 2008) and *The Complete State Security Breach Notification Compliance Handbook* (West 2009). He also serves as Executive Director of Stanford University Law School's Center for E-Commerce, which hosts the annual Best Practices Conference where lawyers, scholars and judges are regularly featured and interact.

Ian was named the Lawyer of the Year for Information Technology Law in the 2019, 2018, 2016 and 2013 editions of Best Lawyers in America and was recognized as the 2012 [New Media Lawyer of the Year](#) by the Century City Bar Association. In 2018 he was recognized by *World Trademark Review* for his trademark litigation practice and was named one of the Top 20 Cyber/Artificial Intelligence Lawyers by the *Los Angeles and San Francisco Daily Journal*. He received the "Trailblazer" Award, Intellectual Property, 2017 from *The National Law Journal* and he has been recognized as a "Groundbreaker" in *The Recorder's* 2017 Litigation Departments of the Year Awards. In 2010 he was the recipient of the State Bar of California IP Section's Vanguard Award for significant contributions to the development of intellectual property law (<http://ipsection.calbar.ca.gov/IntellectualPropertyLaw/IPVanguardAwards.aspx>). He is listed in Legal 500 U.S., The Best Lawyers in America (in the areas of information technology and intellectual property) and Chambers and Partners USA Guide in the areas of privacy and data security and information technology. Mr. Ballon was listed in *Variety's* "Legal Impact Report: 50 Game-Changing Attorneys" and has been named one of the top 100 lawyers in California and has been recognized as one of the Top 75 intellectual property litigators in California by the *Los Angeles and San Francisco Daily Journal* in every year that the list has been published, from 2009 through 2018. He was also recognized as one of the top 100 lawyers in L.A. by the *Los Angeles Business Journal*. He is also listed in Legal 500 U.S., The Best Lawyers in America (in the areas of information technology and intellectual property) and Chambers and Partners USA Guide in the areas of privacy and data security and information technology. Mr. Ballon also holds the CIPP/US certification from the International Association of Privacy Professionals (IAPP).



- 27.08[5] Methods of Notification**
- 27.08[6] The Content and Required Text of Consumer Notices**
- 27.08[7] Additional Notices to Credit Reporting Agencies**
- 27.08[8] Additional or Alternative Notices to State Agencies**
- 27.08[9] The Provision of Credit Monitoring Services to Affected Consumers**
- 27.08[10] Claims, Defenses, Remedies and Sanctions for Non-compliance with Security Breach Notification Laws**
  - 27.08[10][A] In General**
  - 27.08[10][B] State Enforcement**
  - 27.08[10][C] Private Claims for Damages, Injunctive Relief and Attorneys' Fees**
  - 27.08[10][D] Nevada's Statutory Cause of Action Against Data Collectors**
  - 27.08[10][E] Michigan's Phony Notification Criminal Statute**
  - 27.08[10][F] Criminal Sanctions for Willful Disclosures By Government Employees**
  - 27.08[10][G] Student Expulsion Based on A Security Breach**
- 27.08[11] Contractual Waivers of Notice Obligations**
- 27.08[12] Data Destruction and Security Freeze Laws**
- 27.08[13] Compliance Checklist**
- 27.08[14] Additional Rules for Credit and Debit Card Account Information**
- 27.09 Catalogue of State and Territorial Security Breach Notification Statutes**
  - 27.09[1] Overview**
  - 27.09[2] Alabama**
  - 27.09[3] Alaska**
  - 27.09[4] Arizona**

## 27.08 Analysis of State Security Breach Notification Statutes

### 27.08[1] Overview and Strategic Considerations

All fifty states, the District of Columbia, Puerto Rico, Guam and the U.S. Virgin Islands have security breach notification statutes in effect.<sup>1</sup> Financial institutions subject to the Gramm-Leach-Bliley Act may also be required to provide notice to consumers of security breaches in certain circumstances.<sup>2</sup> Health care providers and others similarly may have notification obligations under the Recovery and Reinvestment Act of 2009 when medical records have been compromised.<sup>3</sup> In addition, the Securities and Exchange Commission issued a disclosure guidance document in October 2011<sup>4</sup> that public companies should consider if they experience a security breach.<sup>5</sup> As separately analyzed in section 27.07, the failure to provide notice also may form the basis for negligence, breach of fiduciary duty or other claims in litigation. This section (27.08) analyzes security breach notification obligations under U.S. state and territorial statutes. State laws mandating that companies maintain reasonable security measures and other safeguards to minimize the risk of a security breach are analyzed in section 27.04[6][C]. State data minimization laws mandating the destruction or deletion of personal information are separately analyzed in section 27.04[6][D]. The following section (27.09) reprints the security breach notification laws analyzed in this section and the data safeguard and minimization statutes analyzed in section 27.04[6].

The particular language used in a given state statute, and the nature of the undertaking required, often depends on when a state statute was first enacted or most recently

---

#### [Section 27.08[1]]

<sup>1</sup>A compendium of the security breach notification statutes and implementing regulations adopted as of November 2018 to take effect on or by January 1, 2019 in each state and territory is set forth in section 27.09. With the adoption of security breach notification statutes by Alabama and South Dakota in 2018, by July 1 of that year, every state had enacted some form of security breach notification statute.

<sup>2</sup>*See supra* § 27.04[3][C].

<sup>3</sup>*See supra* § 27.04[4].

<sup>4</sup>U.S. Securities and Exchange Commission, Division of Corporation Finance, CF Disclosure Guidance: Topic 2—Cybersecurity (Oct. 13, 2011).

<sup>5</sup>*See supra* § 27.04[5][B].

amended. Those enacted or amended most recently typically impose more detailed and specific requirements, reflecting the collective experience of legislators and regulators across the country in better understanding the nature of security breaches today and assessing what risks to consumers they believe could require notice.

The first security breach notification statute, enacted in **California**, became effective in 2003. As a result of that law, Choicepoint, a large data broker, revealed in early 2005 that it had sold personal information about more than 140,000 consumers to identity thieves who had posed as legitimate customers. This disclosure, and other publicized security breaches around the same time, created heightened concern about data security which, in turn, led to a majority of the other states to follow California's lead and adopt similar security breach notification statutes. There have also been proposals for federal legislation, although to date none has been enacted.

State and territorial security breach notification statutes and implementing regulations<sup>6</sup> apply to individuals, business entities and/or state agencies. Additional notification obligations may be imposed under the Gramm-Leach-Bliley Act<sup>7</sup> or other federal laws, although a minority of jurisdictions exempt entities subject to other notification obligations from having to also provide notice under state law.

---

<sup>6</sup>In addition to statutory provisions, **Louisiana** has authorized its attorney general to promulgate rules on security breach notification. The most current version of these regulations (which are codified at La. Admin. Code tit. 16, § 701 (2007)) is set forth in section 27.09[21] and discussed in this section. **Massachusetts** also authorized regulations adjusting as needed the definition of the strength of acceptable encryption. See Mass. Gen. L. Ann. Ch 93H §§ 2 (directing the department of consumer affairs and business regulation to promulgate regulations), 1(a) (defining *encrypted* "unless further defined by regulation of the department of consumer affairs and business regulation."); 201 Mass. Code Regs. §§ 17.01 to 17.05. The **New Jersey** legislature also has authorized implementing regulations. See N.J. Stat. Ann. § 56:8-165. In addition, **Puerto Rico**'s notification statute implicitly anticipates that implementing regulations could issue in authorizing fines for violations of the statute "or its regulations." 10 P.R. Stat. § 4055. Other jurisdictions may issue regulations as well in the future. Practitioners should therefore review the website of the applicable consumer affairs or equivalent agency responsible for a given state's implementation of its security breach notification statute in seeking to comply with that state's law.

<sup>7</sup>Separate notification requirements under that statute are set forth in section 27.04[3][C].

Most statutes are modeled on California's original security breach notification law, although as more states have enacted their own statutes and subsequently revised them, the number of variations in state laws has increased (and even California has amended its original statute several times). The challenge for businesses that must respond to security breach notification obligations for residents of all U.S. states and territories is to navigate through legal obligations that are slightly different in a number of jurisdictions and in some instances impose conflicting disclosure requirements.

When a breach first occurs, a company must consider whether to contact law enforcement (and, if so, which agency), based on the nature of the breach and applicable law, and quickly evaluate how to investigate the nature of the breach.<sup>8</sup> A business also should evaluate both the legal consequences of the breach and its PR consequences. All of these issues are best considered in advance, rather than at the time a breach first occurs, to be able to respond strategically and proactively.

Not all security breaches require notification. For example, even breaches that expose confidential or highly sensitive data or information may not trigger notification obligations (depending on the data elements involved in the breach). Conversely, a breach that involves seemingly innocuous information may trigger notification obligations in some jurisdictions. In fact, if particular data elements have been compromised (such as a person's name and Social Security number) notification may be required even if the affected person, company or government agency is not certain that a breach actually occurred.<sup>9</sup> Regardless of the data elements exposed, notification may not be required in certain circumstances if they were encrypted or redacted or otherwise rendered unusable,<sup>10</sup> at least under some state security breach notification laws. Even when not required, some businesses choose to provide notice as a service to their customers, in the expectation that the breach may come to light one day and their silence could create public relations issues, or to avoid potential claims of negligence or breach of implied

---

<sup>8</sup>Some of these considerations are outlined in chapter 43, which addresses strategic responses to data theft.

<sup>9</sup>*See infra* § 27.08[3].

<sup>10</sup>*See infra* § 27.08[3][C].

contract (or similar theories) for failing to warn or otherwise take action.<sup>11</sup>

In the event of a possible security breach, an affected business<sup>12</sup> must first determine which state laws in fact apply based on the residence<sup>13</sup> of affected persons (and in some instances also the state(s) where the company operates).<sup>14</sup>

---

<sup>11</sup>See, e.g., *In re TJX Cos. Retail Security Breach Litig.*, 564 F.3d 489, 495–98 (1st Cir. 2009) (reversing the lower court’s dismissal of plaintiffs’ unfair trade practices claim under Massachusetts law, where the company’s conduct allegedly was systematically reckless and aggravated by a failure to give prompt notice when lapses were discovered internally, which allegedly caused widespread and serious harm to other companies and consumers); *In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d 518, 531–32 (N.D. Ill. 2011) (holding that plaintiffs stated a claim for implied contract based on the existence of an implicit contractual relationship between plaintiffs and Michaels obligating Michaels to take reasonable measures to protect plaintiffs’ financial information and notify plaintiffs of a security breach within a reasonable amount of time); see generally *supra* § 27.07 (analyzing claims raised in litigation).

<sup>12</sup>Although many state security breach notification laws also apply to agencies, as a practical matter state agencies typically deal with security breaches that only involve state residents or the law of a single state, whereas business entities and potentially individuals may own data elements of residents of multiple jurisdictions. **Alaska**’s statute applies to a person doing business, a government agency or a person with more than 10 employees. Alaska Stat. § 45.48.090(2).

<sup>13</sup>Although most statutes are silent on this point, absent additional information, a person’s residence generally may be presumed to correspond to his or her mailing address. **Pennsylvania** expressly provides that “an individual whose principal mailing address, as reflected in the computerized data which is maintained, stored or managed by the entity,” is in Pennsylvania, is deemed to be a resident. 73 Pa. Stat. Ann. § 2303(a). **Ohio** uses substantially the same definition, providing that “a resident of this state is an individual whose principal mailing address as reflected in the records of the person is in this state.” Ohio Rev. Code Ann. § 1349.19(B)(1).

<sup>14</sup>For example, **Wisconsin** obligates entities whose principal place of business is located in Wisconsin to provide notice to all affected persons, while out-of-state entities are merely required to notify state residents. See Wis. Stat. Ann. § 134.98(2).

**Texas** similarly obligates a person who conducts business in the state and owns or licenses computerized data that includes sensitive personal information to provide notice to “any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person” except residents of states that would require notice to be sent. Tex. Bus. & Com. Code Ann. §§ 521.053(b), 521.053(b-1) (emphasis added). While previously this meant that persons or entities that conducted business in Texas had to send notice to residents of Texas

Where a potential data breach involves residents of only a small number of states, lawyers should review the applicable state statutes and regulations (which are set out in alphabetical order in section 27.09) to determine the best potential response for their clients. The balance of section 27.08, while focused on obligations from a national perspective, nonethe-

---

and residents of those states that did not otherwise have security breach notification laws in effect, since July 1, 2018, when the security breach notification law of the last state to have one take effect (South Dakota) became effective, Texas law effectively only requires notice to Texas residents. The law is unclear, however, about whether notice would be required to residents of states whose own breach notification laws would not compel notice in circumstances where the Texas law would. In such cases, there could be dormant Commerce Clause limitations on the extent to which Texas could enforce its law to apply to non-residents (as well as questions about what level of activity is required to constitute conducting business in the state). *See infra* §§ 35.04, 35.05 (analyzing dormant Commerce Clause restrictions on state regulation of Internet commerce).

**California's** statute applies to any individual, commercial entity or state agency that conducts business in the state and owns or licenses computerized data that includes personally identifying information about a state resident (1) whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person, or (2) whose encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person and the agency that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that personal information readable or useable. Cal. Civ. Code §§ 1798.82(a) (individuals and entities), 1798.29(a) (state agencies); *see also, e.g.*, Conn. Gen. Stat. Ann. § 36a-701b(b) (obligating any person or entity conducting business in **Connecticut** who, in the ordinary course of business, owns, licenses or maintains data, to provide notice to state residents whose personal information was breached, or is reasonably believed to have been breached); N.M. Stat. Ann. §§ 57-12C-2(D), 57-12C-6(A) (requiring notice to a **New Mexico** resident when personally identifying information “is reasonably believed to have been subject to a security breach,” which in turn is defined (subject to exceptions) as “the unauthorized acquisition of unencrypted computerized data, or of encrypted computerized data and the confidential process or key used to decrypt the encrypted computerized data, that compromises the security, confidentiality or integrity of personal identifying information maintained by a person”). **Wyoming's** statute applies to persons or entities doing business in the state that own or license computerized data that includes personally identifying information about a Wyoming resident. Wyo. Stat. Ann. § 40-12-502(a). **Mississippi** modifies the provision to reach “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 . . . .” Miss. Code Ann. § 75-24-29(1) (emphasis added).

less includes practice tips that may be helpful even in individual cases. Comparing the text of a particular state's security breach notification statute with those enacted in other jurisdictions, as discussed throughout the balance of section 27.08, may also be useful in responding in individual cases.

Broader consideration will be required if data or information about residents of numerous states has been compromised. Subsections 27.08[2] through 27.08[13] lay out the requirements, exemptions, remedies and sanctions imposed by all U.S. state and territorial laws. These subsections follow the California statute that serves as the model for most other laws, pointing out differences that exist under particular state and territorial laws. The objective of this section is to allow lawyers to quickly and easily evaluate notification obligations under all potentially applicable laws and then adequately respond to a breach.

Where a fifty-state response is required, lawyers must evaluate how to address those laws that potentially conflict with one another. Most pronounced is the requirement under **Massachusetts** law that the details of the nature of the breach not be disclosed to Massachusetts residents, while the laws of multiple states mandate this very disclosure.<sup>15</sup>

Some state laws may make it desirable (but not mandatory) for businesses to tailor notices to residents of particular states, rather than sending the same communication to all U.S. residents. For example, the **Maryland** security breach notification statute requires that the full contact information for the Maryland Attorney General be included in all letters sent to state residents<sup>16</sup> (which may be difficult to do in a single national letter unless similar information is provided for the Attorneys General of all other states and territories, which lengthens the text of the notice letter or the size of attachments). Similarly, Massachusetts law requires that the specific cost of placing a security freeze on a Massachusetts resident's credit report be set forth in a notice letter sent to state residents. Prior to 2018, when a federal statute eliminated charges for credit freezes, it would have been difficult to provide this information in a single letter sent to all U.S. residents (short of including a fee schedule for every U.S. jurisdiction, even though disclosure of this information was not required for residents of most states).

---

<sup>15</sup>See *infra* § 27.08[6].

<sup>16</sup>See Md. Code Ann., Com. Law § 14-3504(g)(4)(i)(2).

The time for providing notice under different state laws also may create conflicts that require special attention. Although phrased somewhat differently, most statutes require that notice be sent without undue delay. Some statutes provide exceptions that allow for delay to accommodate law enforcement (so that notice does not jeopardize an ongoing investigation) or to allow a company to correct any security flaws (so that the notice does not invite further successful attacks). Approximately 17 states, including **Colorado, Florida, Maine** and **Ohio**, have fixed deadlines (as short as 30 days) by which time notice must be sent (and in the case of Florida, the failure to meet the deadline can trigger daily fines up to a maximum of \$500,000).<sup>17</sup> Yet, some other state statutes prohibit notice from being sent until police approval has been obtained.<sup>18</sup> In these circumstances, a person or entity theoretically could choose to provide notice to residents of some states, while withholding it from residents of other states (although this could create public relations problems since some affected residents would likely learn about the breach on blogs or in the press but not actually receive notice until much later and in the intervening period complain to the company or in posts online). Alternatively, a business may defer to the laws of the state where the breach occurred. Thus, for example, if police approval is required in one state but the breach is actually being investigated by police in a different jurisdiction, the inability to get police sign off should not necessarily be viewed as an obstacle to providing notice if the police investigating the breach do not object to notice being sent. Conversely, if delay is mandated by virtue of one state's laws, the delay may not necessarily constitute a violation in the majority of states whose statutes use some form of reasonable (but unspecified) time for a response. In jurisdictions where a hard deadline is imposed, it may also be possible to approach regulators for guidance if the police in another jurisdiction insist that notice be deferred. Ultimately, timing conflicts can be among the trickiest that lawyers have to navigate through in seeking to comply with multiple security breach notification statutes.

Some differences among state and territorial laws largely reflect subtle nuances in draftsmanship that will only rarely be material. For example, **Ohio** excludes information

---

<sup>17</sup>See *infra* § 27.08[4].

<sup>18</sup>See *infra* § 27.08[4].

compiled in news reports, but this category of information is really just a sub-set of the broader category of publicly available information included in most notification statutes.<sup>19</sup> Similarly, the threshold level of risk at which point notification must be made varies under different statutes, ranging from reasonable belief to actual knowledge,<sup>20</sup> but if a company knows that a substantial breach has occurred these different standards will not be meaningful. In addition, as noted above, the length of time required for disclosure and the grounds for delay similarly vary in some respects and are phrased in analogous but not identical ways<sup>21</sup> that may be significant in isolated cases but often may not be material. Needless to say, even small distinctions among state statutes could be significant in individual cases—especially if not taken into account at the outset before notice is sent and instead addressed after the fact in the context of litigation or a regulatory action for breach of a particular notification statute.

Other variations among state and territorial laws are the product of the particular policy preferences of individual state legislators that may be important in localized breaches but may not be material to a company responding on a nation-wide basis. For example, several states require that notice be provided if an account number or the accompanying security code, access code or password is disclosed, while other statutes only require disclosure where both have been exposed.<sup>22</sup> Some states exempt disclosure of a breach that exposed four or five digits from a Social Security or account number (if those are the last digits, any sequence in order, or merely a set number of digits, depending on applicable law).<sup>23</sup> Similarly, **California** and a number of states compel notification where unencrypted material has been accessed without authorization, whereas other states do not require notification if the material, while unencrypted, is redacted or

---

<sup>19</sup>See *infra* § 27.08[3][F].

<sup>20</sup>See *infra* § 27.08[3][A].

<sup>21</sup>See *infra* § 27.08[4].

<sup>22</sup>See *infra* § 27.08[3][B].

<sup>23</sup>Jurisdictions that have one of these variations in their notification statutes include **Guam, Hawaii, Kansas, North Carolina, Pennsylvania, Vermont, West Virginia** and **Wyoming**.

otherwise cannot be used to commit fraud or identity theft.<sup>24</sup> Perhaps more profoundly, **Massachusetts** and **Rhode Island** define encryption to mean 128-bit encryption, whereas weaker forms of encryption would be sufficient to avoid notification in other states (subject to the caveat that some state statutes require notice even where encryption is used if it is likely (for example, because weak encryption was used that would be easy to crack) that the information will be misused).<sup>25</sup> These differences can be significant under an individual or a small number of applicable statutes, but may be less important for a company adopting a uniform response in all jurisdictions.

Some differences among state statutes may only be relevant in particular cases. For example, medical records, health insurance information, biometric and license plate information data are included in the definition of data elements in a small number of states, but would not trigger notification obligations under most state laws.<sup>26</sup> Likewise, while most statutes apply exclusively to electronic data breaches, some compel notification where paper or non-electronic records containing covered data elements have been exposed.<sup>27</sup> In these type of cases, businesses must consider whether to provide notice to all affected persons, regardless of their residency (on the assumption that notice to some would lead to publicity or comments on blogs that could cause public relations problems in states where notice is not provided), or only as, and to the extent, required in particular states. Usually the decision turns on a company's corporate culture, risk tolerance and ability to absorb costs.

Businesses that operate on a nationwide basis may opt to provide notice based on the broadest definition of "personal information" found in any single state statute, pursuant to the most restrictive means of providing notice permitted in all states. This sometimes saves the added cost of closely analyzing and tailoring responses for residents of each jurisdiction, while also providing uniformity (to the extent possible in light of potentially conflicting obligations noted above) to avoid any adverse publicity or comments in the blogosphere about unequal treatment provided to residents

---

<sup>24</sup>See *infra* § 27.08[3][C].

<sup>25</sup>See *infra* §§ 27.08[3][A], 27.08[3][C].

<sup>26</sup>See *infra* § 27.08[3][B].

<sup>27</sup>See *infra* § 27.08[3][E].

of different jurisdictions. These companies may also voluntarily provide credit monitoring services, as discussed below in section 27.08[9]. As discussed in that subsection, identity theft prevention and mitigation services, such as credit monitoring, may be required for Connecticut and Delaware residents.<sup>28</sup> In addition, although other states do not require that these services be provided, if they are, California and Oregon law requires that specific notices about these services be included in certain security breach notification letters sent to state residents.<sup>29</sup>

Other companies seek to do no more than what is required in any given jurisdiction (and to provide no notice at all in states that do not require it), also often driven by cost considerations and concern about the potentially adverse consequences of notifying more people than is absolutely necessary.

Some businesses simply prefer to provide notices tailored to individual states for marketing reasons or to save the cost of mailing physical letters in those jurisdictions where email is permissible.<sup>30</sup>

For similar reasons, a business may elect to provide substitute notice, rather than individual notice, if it is eligible to do so.<sup>31</sup>

In recent years, state legislatures have made a number of technical revisions to their security breach notification laws. It is possible that individual states may make further changes during the course of the year before an updated version of this chapter is released.

In all cases, the text of the actual statutes at issue should be closely reviewed.

Where a breach involves a lawyer or law firm, the ABA has opined that the Model Rules of Professional Conduct require that a lawyer notify clients and take other reasonable steps to protect client interests.<sup>32</sup>

Even before a breach has happened, counsel and IT profes-

---

<sup>28</sup>See Conn. Gen. Stat. Ann. § 36a-701b(b)(2)(B); Del. Code Ann. tit. 6, § 12B-102(e); *see generally infra* § 27.08[9].

<sup>29</sup>See Cal. Civ. Code § 1798.82(d)(2)(H); Or. Rev. Stat. Ann. § 646A.604(7); *see generally infra* § 27.08[9].

<sup>30</sup>See *infra* § 27.08[5].

<sup>31</sup>See *infra* § 27.08[5].

<sup>32</sup>See *Lawyers' Obligations After an Electronic Data Breach or Cyber-*

sionals should assess a company's security risks and map out potential strategies for responding in the event of a breach. Both electronic breaches (such as hacker attacks) and traditional physical security breaches (such as break-ins at a company's offices or the loss or theft of a laptop) can trigger security breach notification obligations. Pre-planning, including table top exercises, and employee education can go a long way towards preventing a breach and reducing costs and potential mistakes, in the event of a breach.

Individuals, businesses and agencies that think through these issues in advance also may provide notice pursuant to an information security policy, as discussed at greater length in section 27.11.

After a breach occurs, the affected company may be subject to FTC and state Attorneys General regulatory enforcement actions and potentially litigation, including class action litigation, depending on the nature and circumstances of the breach, the extent to which it could have been prevented, and a company's pre-breach representations about the state of its security.<sup>33</sup> While notice to regulators and consumers can accelerate these problems, failing to properly and timely comply with state security breach notification obligations can only compound them.

### 27.08[2] Persons Obligated to Provide Notice

Most state statutes apply to persons, companies and/or government agencies that own or license computerized data that includes personal information (or have access to it on behalf of owners and licensees), although some state laws such as the one in effect in **Washington** apply more broadly to data (whether or not computerized).<sup>1</sup> **Vermont's** law applies expressly to data brokers,<sup>2</sup> who are not only required to disclose a breach to the extent they constitute *data collectors*

---

attack, ABA Formal Opinion 483 (Oct. 17, 2018).

<sup>33</sup>These issues are addressed in other sections in this chapter, including section 27.01.

#### [Section 27.08[2]]

<sup>1</sup>See Wash. Rev. Code Ann. § 19.255.010(1); Wash. Rev. Code Ann. § 42.56.590(1)(a).

<sup>2</sup>See Vt. Stat. Ann. tit. 9, §§ 2430, 2446; see generally *supra* § 27.04[6][J]. A *data broker* is "a business, or unit or units of a business, separately or together, that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom

under state law,<sup>3</sup> but in connection with their obligation to register annually with the Vermont Secretary of State must disclose the number of security breaches they have experienced in the prior year and, if known, the total number of consumers affected by the breach.<sup>4</sup> In general, persons or

---

the business does not have a direct relationship.” Vt. Stat. Ann. tit. 9, § 2430(4)(A). Examples of a *direct relationship* with a business include “if the consumer is a past or present: (i) customer, client, subscriber, user, or registered user of the business’s goods or services; (ii) employee, contractor, or agent of the business; (iii) investor in the business; or (iv) donor to the business.” *Id.* § 2430(4)(B). The statute provides that “the following activities conducted by a business, and the collection and sale or licensing of brokered personal information incidental to conducting these activities, do not qualify the business as a data broker: (i) developing or maintaining third-party e-commerce or application platforms; (ii) providing 411 directory assistance or directory information services, including name, address, and telephone number, on behalf of or as a function of a telecommunications carrier; (iii) providing publicly available information related to a consumer’s business or profession; or (iv) providing publicly available information via real-time or near-real-time alert services for health or safety purposes.” *Id.* § 2430(4)(C). The phrase *sells or licenses* does not include: “(i) a one-time or occasional sale of assets of a business as part of a transfer of control of those assets that is not part of the ordinary conduct of the business; or (ii) a sale or license of data that is merely incidental to the business.” *Id.* § 2430(4)(D).

<sup>3</sup>A *data collector* is “a person who, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates, or otherwise deals with personally identifiable information, and includes the State, State agencies, political subdivisions of the State, public and private universities, privately and publicly held corporations, limited liability companies, financial institutions, and retail operators.” Vt. Stat. Ann. tit. 9, § 2430(6).

<sup>4</sup>Vt. Stat. Ann. tit. 9, § 2446(a)(3)(E); *see generally supra* § 27.04[6][J]. A *data broker security breach* means “an unauthorized acquisition or a reasonable belief of an unauthorized acquisition of more than one element of brokered personal information maintained by a data broker when the brokered personal information is not encrypted, redacted, or protected by another method that renders the information unreadable or unusable by an unauthorized person.” Vt. Stat. Ann. tit. 9, § 2430(5)(A). The definition excludes, however, “good faith but unauthorized acquisition of brokered personal information by an employee or agent of the data broker for a legitimate purpose of the data broker, provided that the brokered personal information is not used for a purpose unrelated to the data broker’s business or subject to further unauthorized disclosure.” *Id.* § 2430(5)(B). In determining whether brokered personal information has been acquired or is reasonably believed to have been acquired by a person without valid authorization, “a data broker may consider the following factors, among others: (i) indications that the brokered personal information is in the physical possession and control of a person without valid authorization, such as a lost or stolen computer or other device containing brokered

entities that maintain data that they do not own (under some statutes, *a third-party agent or service provider*<sup>5</sup>), if any, must provide notice to owners or licensees (in some states, *covered entities*<sup>6</sup>),<sup>7</sup> who, based on notice or their own knowledge of a breach, must provide notice to consumers (either when they get notice of a breach or discover it independently) and potentially state agencies and/or credit reporting agencies. For example, **Illinois** law requires that a data collector that owns or licenses personal information concerning an Illinois resident notify the resident, while data collectors that maintain or store but do not own or license computerized data that includes personal information must notify the owner or licensee and cooperate with the owner” in matters relating to the breach” including, but not limited to, (i) informing the owner or licensee of the breach, including “giving notice of the date or approximate date of the breach and the nature of the breach, and (ii) informing the owner or li-

---

personal information; (ii) indications that the brokered personal information has been downloaded or copied; (iii) indications that the brokered personal information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported; or (iv) that the brokered personal information has been made public.” *Id.* § 2430(5)(C).

<sup>5</sup>A *third party agent* is defined under Alabama law as an “entity that has been contracted to maintain, store, process, or is otherwise permitted to access sensitive personally identifying information in connection with providing services to a covered entity.” Ala. Code § 8-38-2(7). Under Colorado law, a *third-party service provider* means “an entity that has been contracted to maintain, store, or process personal information on behalf of a covered entity.” Colo. Rev. Stat. Ann. § 6-1-716(1)(1). Under Florida law, a *third-party agent* is “an entity that has been contracted to maintain, store, or process personal information on behalf of a covered entity or governmental entity.” Fla. Stat. Ann. § 501.171(1)(h).

<sup>6</sup>A *covered entity* is defined under Alabama law, for example, as a “person, sole proprietorship, partnership, government entity, corporation, nonprofit, trust, estate, cooperative association, or other business entity that acquires or uses sensitive personally identifying information.” Ala. Code § 8-38-2(2). Under Colorado law the term is defined to mean a person “that maintains, owns, or licenses personal information in the course of the person’s business, vocation or occupation.” Colo. Rev. Stat. Ann. § 6-1-716(1)(1)(i). Under Florida law it is “a sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity that acquires, maintains, stores, or uses personal information.” Fla. Stat. Ann. § 501.171(1)(b).

<sup>7</sup>*See, e.g.,* Fla. Stat. Ann. § 501.171(6) (“In the event of a breach of security of a system maintained by a third-party agent, such third-party agent shall notify the covered entity of the breach of security as expeditiously as practicable, but no later than 10 days following the determination of the breach of security or reason to believe the breach occurred.”).

censee of any steps the data collector has taken or plans to take relating to the breach.”<sup>8</sup> Similarly, **Kentucky** law provides that “[a]ny information holder that maintains computerized data that includes personally identifiable information that the information holder does not own shall notify the owner or licensee of the information of any breach of the security of the data as soon as reasonably practicable following discovery,” if the personally identifiable information was, or is reasonably believed to have been, acquired by an unauthorized person.<sup>9</sup> **South Dakota**’s law likewise applies to information holders.<sup>10</sup>

While most statutes apply to persons, companies and/or government agencies, the law enacted in **Maine** generally<sup>11</sup> applies more narrowly only to *information brokers*. The **Illinois**, **Nevada** and **Vermont** statutes apply more broadly to *data collectors*,<sup>12</sup> while **Georgia** applies to both data collec-

---

<sup>8</sup>815 Ill. Comp. Stat. Ann. §§ 530/10(a), 530/10(b). The statute further provides that “[t]he data collector’s cooperation shall not, however, be deemed to require either the disclosure of confidential business information or trade secrets or the notification of an Illinois resident who may have been affected by the breach.” *Id.* § 530/10(b).

<sup>9</sup>Ky. Rev. Stat. Ann. § 365.732(3).

<sup>10</sup>See S.D. Codified Laws § 22-40-19(3) (defining an *information holder* as “any person or business that conducts business in this state, and that owns or licenses computerized personal or protected information of residents of this state . . .”).

<sup>11</sup>Maine requires notice by persons who are not information brokers only if the person determines that misuse of the personal information has occurred, or is reasonably possible that misuse will occur. Me. Rev. Stat. Ann. tit. 10, § 1348 (1)(B).

<sup>12</sup>A *data collector* under Illinois law “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.” 815 Ill. Comp. Stat. Ann. § 530/5. The term is similarly defined (although without the more expansive “include, but is not limited to” language) under Nevada law. See Nev. Rev. Stat. § 603A.030.

Under Vermont law, data collector was defined the same way as in Illinois, but with somewhat broader reference to state agencies and political subdivisions, but the definition was revised further effective January 1, 2019. See Vt. Stat. Ann. tit. 9, § 2430(6). Prior to 2012, Vermont effectively excluded Vermont law enforcement agencies from its definition of this term in Vt. Stat. Ann. tit. 9, § 2435(h), which was repealed in 2012. A *data collector* means “a person who, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates, or

tors and information brokers.<sup>13</sup> **Wisconsin**'s notification statute applies to entities (but not individuals) that conduct business in the state and "maintain personal information in the ordinary course of business," license personal information in Wisconsin, maintain for a state resident a depository account or lend money to a state resident.<sup>14</sup> **Alaska**'s statute compels notice by *covered persons*, which is defined to mean a person doing business, a government agency or a person with more than ten employees.<sup>15</sup> **Puerto Rico**'s security breach statute previously applied to proprietors or custodians of data banks for commercial use, and resellers and providers of access to digital data banks that include personal information of residents of Puerto Rico, but was amended to apply to owners or custodians of databases that include personal information of residents of Puerto Rico (and resellers and access providers).<sup>16</sup>

**Kentucky**'s security breach statute governing breaches by a person or business is similarly broad, applying to any *in-*

---

otherwise deals with personally identifiable information, and includes the State, State agencies, political subdivisions of the State, public and private universities, privately and publicly held corporations, limited liability companies, financial institutions, and retail operators." Vt. Stat. Ann. tit. 9, § 2430(6). As noted earlier in this subsection, Vermont's security breach notification law applies expressly to *data brokers*. See Vt. Stat. Ann. tit. 9, §§ 2430, 2446; see generally *supra* § 27.04[6][J].

<sup>13</sup>An *information broker* is defined under Georgia law as:

A person or entity who, for monetary fees or dues, engages in whole or in part in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring, or communicating information concerning individuals for the primary purpose of furnishing personal information to nonaffiliated third parties, but does not include any governmental agency whose records are maintained primarily for traffic, safety, law enforcement, or licensing purposes.

Ga. Code Ann. § 10-1-911(3). Maine law includes substantially the same definition. See Me. Rev. Stat. Ann. tit. 10, § 1347(3).

A *data collector* under Georgia law means

any state or local agency or subdivision thereof including any department, bureau, authority, public university or college, academy, commission, or other government entity; provided, however, that the terms 'data collector' shall not include any governmental agency whose records are maintained primarily for traffic safety, law enforcement, or licensing purposes or for purposes of providing public access to court records or to real or personal property information.

Ga. Code Ann. § 10-1-911(2).

<sup>14</sup>Wis. Stat. Ann. § 134.98(1)(a).

<sup>15</sup>Alaska Stat. §§ 45.48.010, 45.48.090(2).

<sup>16</sup>10 L.P.R. Ann. § 4052. While modeled on other security breach notification statutes, Puerto Rico's statute initially used unique terminology that was not found in the laws of other U.S. jurisdictions.

*formation holder*, which is defined as any person or business entity that conducts business in Kentucky.<sup>17</sup>

Kentucky also enacted a separate statute governing breaches by government agencies and educational institutions.<sup>18</sup> That statute also applies to *nonaffiliated third parties*, who are contractors who receive personal information from an agency.<sup>19</sup> A nonaffiliated third party generally is required to notify the agency from which it obtained access to personal information of a breach within 72 hours of discovery of the breach.<sup>20</sup>

**Montana** imposes a notification obligation on owners, licensees and insurance-support organizations.<sup>21</sup>

**Connecticut** also imposes notification obligations (as well as affirmative obligations to maintain and safeguard the security of information) on state government contractors.<sup>22</sup>

Although the terminology used in individual statutes varies somewhat, most security breach notification statutes require owners or licensees of computerized data that includes personally identifying information to give notice to affected consumers and require entities that maintain but do not own data to give notice to the owner or licensee. Notification obligations typically are imposed on individuals and entities and, in some states, governmental agencies.<sup>23</sup> As discussed below in sections 27.08[7] and 27.08[8], notice to

---

<sup>17</sup>Ky. Rev. Stat. Ann. § 365.732(1)(b).

<sup>18</sup>See Ky. Rev. Stat. Ann. §§ 61.931 *et seq.*

<sup>19</sup>See Ky. Rev. Stat. Ann. § 61.931(5).

<sup>20</sup>See Ky. Rev. Stat. Ann. § 61.932.

<sup>21</sup>See Mont. Code Ann. § 30-14-1704(a); Mont. Code Ann. § 33-19-321.

<sup>22</sup>See Conn. Gen. Stat. Ann. § 15-142.

<sup>23</sup>Those jurisdictions whose security breach notification statutes apply in whole or part to government agencies include: **Alaska, California, Florida, Guam, Georgia, Idaho, Illinois, Indiana, Kansas, Kentucky, Maryland, Massachusetts, Michigan, Minnesota, Montana, Nevada, New York, Ohio, Oklahoma, Rhode Island** (both state and municipal agencies), **South Carolina, Tennessee, Vermont, the U.S. Virgin Islands, Washington and Wisconsin.**

Minnesota's statute also applies to data "maintained by a person under a contract with the government entity that provides for the acquisition or access to the data by an employee, contractor, or agent of the government entity." Minn. Stat. Ann. § 13.055(1)(a).

Some states, such as Kentucky, explicitly include public schools and public post-secondary educational institutions. See Ky. Rev. Stat. Ann. §§ 61.931(a)(1)(d), 61.931(a)(1)(e).

credit reporting bureaus and state agencies may also be required.

Some, but not all, statutes exempt entities otherwise subject to notification obligations under the Gramm-Leach-Bliley Act,<sup>24</sup> the Health Insurance Portability and Accountability Act (HIPAA)<sup>25</sup> or other laws.<sup>26</sup> Even where notice

<sup>24</sup>See *supra* § 27.04[3].

<sup>25</sup>See *supra* § 27.04[4].

<sup>26</sup>States and territories with these type of exemptions include: **Alabama** (any entity subject to or regulated by federal laws, regulations, procedures, or guidance, on data breach notification, which maintains procedures pursuant to those directions, provides notice to affected individuals pursuant to those directions, and timely provides a copy of the notice to the state Attorney General when the number of individuals notified by the entity exceeds 1,000); **Arizona** (any person subject to Gramm-Leach-Bliley Act and covered entities and business associates within the meaning of HIPAA); **Arkansas** (general exemption for any person or business subject to equivalent or greater security and notification obligations under state or federal law); **California** (covered entities under HIPAA that have complied completely with section 13402(f) of the HITECH Act); **Colorado** (persons subject to Gramm-Leach-Bliley and the same general exemption as under Arkansas law); **Connecticut** (any person that maintains a security breach procedure pursuant to the rules, regulations, procedures or guidelines established by the primary or functional federal regulator); **Delaware** (a person regulated by state or federal law, including HIPAA and Gramm-Leach-Bliley, who is required to provide notice under those laws or implementing regulations); the **District of Columbia** (Gramm-Leach-Bliley); **Florida** (primary or functional federal regulator); **Guam** (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 or 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 regulator); **Hawaii** (financial institutions subject to the Federal Interagency Guidance on Response Programs analyzed in § 27.04[3][C] and any health plan or health care provider subject to the security provisions of HIPAA); Idaho (primary regulator); **Illinois** (data collections in compliance with section 501(b) of Gramm-Leach-Bliley or any covered entity or business associate subject to and in compliance with HIPAA); **Indiana** (institutions subject to Gramm-Leach-Bliley and any person or private entity that maintains its own disclosure procedures as part of an information privacy, security policy or compliance plan under the USA Patriot Act, Executive Order 133224, the Driver's Privacy Protection Act, the Fair Credit Reporting Act, the Financial Modernization Act of 1999 or HIPAA, provided that notice to Indiana residents is made without unreasonable delay pursuant to such policy or plan); **Iowa** (same as Colorado); **Kansas** (any individual or 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 . . . or

guidelines established by its primary or functional state or federal regulator . . . .”); **Kentucky** (Gramm-Leach-Bliley Act and HIPAA); **Louisiana** (financial institutions subject to the Federal Interagency Guidance on Response Programs); **Maryland** (Gramm-Leach-Bliley, the Fair and Accurate Transactions Act, the federal Interagency Guidelines Establishing Information Security Standards, or procedures or guidelines established by the primary or functional federal or state regulator); **Massachusetts** (federal laws, rules, regulations, guidance, or guidelines); **Michigan** (Federal Interagency Guidance or HIPAA); **Minnesota** (“financial institutions” subject to Gramm-Leach-Bliley and entities subject to federal privacy and security regulations adopted pursuant to HIPAA); **Missouri** (state or federal regulation that requires notice to consumers; or a financial institution that is (a) subject to the Federal Interagency Guidance on Response Programs analyzed in § 27.04[3][C], or subject to and in compliance with the National Credit Union Administration regulations, or subject to Gramm-Leach-Bliley); **New Hampshire** (any person or entity that maintains procedures for security breach notification pursuant to guidelines issued by a state or federal regulator); **New Mexico** (any person subject to Gramm-Leach-Bliley or HIPAA); **Nebraska** (primary or functional state or federal regulator); **Nevada** (entities subject to the privacy and security provisions of the Gramm-Leach-Bliley Act); **North Carolina** (financial institutions subject to the Federal Interagency Guidance on Response Programs); **North Dakota** (covered entities under HIPAA); **Ohio** (financial institutions and similar entities required by federal law to notify consumers in the event of a security breach and persons or entities regulated by the Social Security Act); **Oklahoma** (Federal Interagency Guidance on Response Programs or guidelines established by the primary or functional federal regulator; this exception applies only for breaches involving individuals or entities, not state agencies); **Oregon** (a person that complies with (a) notice requirements from its primary or functional federal regulator, (b) state or federal law that provides greater protection to personal information and at least as thorough disclosure requirements for breach of security of personal information than that provided by Oregon law, or (c) Title V of Gramm-Leach-Bliley, or is a covered entity under HIPAA); **Pennsylvania** (financial institutions subject to the Federal Interagency Guidance on Response Programs and entities that comply with the notification requirements or procedures established by the entity’s primary or functional Federal regulator); **Rhode Island** (financial institutions subject to the Federal Interagency Guidance on Response Programs, entities subject to HIPAA, and persons who maintain a security breach procedure pursuant to rules, regulations or guidelines established by the primary or functional regulator); **South Carolina** (section 39-1-90, applicable to persons but not agencies, exempts banks or financial institutions subject to the Gramm-Leach-Bliley Act and financial institutions subject to and in compliance with the federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice); **South Dakota** (Health Insurance Portability and Accountability Act of 1996, Gramm Leach Bliley Act, laws, rules, regulations, guidance, or guidelines established by an information holder’s primary or functional federal regulator); **Tennessee** (Gramm-Leach-Bliley and HIPAA); **Utah** (persons

under state law is exempted on this basis, notice to the state that consumer notice pursuant to these other laws has been provided may be required.<sup>27</sup>

Most states also allow entities to maintain their own notification procedures as part of an information security policy, in lieu of complying with the specific provisions of the statute.<sup>28</sup> For residents of some states, however, persons or entities that provide notice to consumers pursuant to their own information security policies may nevertheless be required to also notify the Attorney General or another state agency to advise when notice to consumers pursuant to their policy has been sent.<sup>29</sup>

In addition to notice obligations imposed on other persons or entities, **Vermont** requires any law enforcement agency with a reasonable belief that a security breach has or may have occurred at a specific business to notify the business in writing of its belief.<sup>30</sup>

---

who maintain security breach systems established by the primary state or federal regulator); **Vermont** (financial institutions subject to the Federal Interagency Guidance on Response Programs or 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); **Virginia** (an entity subject to Gramm-Leach-Bliley or that complies with notification requirements or procedures established by the entity's primary or functional state or federal regulator); **Washington** (a covered entity under HIPAA, a financial institution under the authority of the Office of the Comptroller of the Currency, the FDIC, the National Credit Union Administration or the Federal Reserve System, subject to various conditions); **West Virginia** (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 or 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, and a covered entity under HIPAA); **Wisconsin** (Gramm-Leach-Bliley and HIPAA); and **Wyoming** (Gramm-Leach-Bliley, specifically financial institutions or federal credit unions subject to the requirements of 15 U.S.C.A. § 6801(b)(3) and 12 C.F.R. Part 364 Appendix B or Part 748 Appendix B).

<sup>27</sup>See *infra* § 27.08[8].

<sup>28</sup>See *supra* § 27.08[1]; see generally *infra* § 27.08[11].

<sup>29</sup>See *infra* § 27.08[8].

<sup>30</sup>Vt. Stat. Ann. tit. 9, § 2435(4)(B). The agency is also required to notify the business that additional information on the security breach may need to be furnished to the Office of the Attorney General or the Department of Financial Regulation and shall include the website and

### 27.08[3] Breaches that Trigger Notification Obligations

#### 27.08[3][A] In General

Whether notice must be sent depends in part on whether a breach has or is believed to have occurred and in some cases the potential consequences of the breach. If a breach has occurred, a number of states require that notice be provided within a set period of time, which may be as short as 30 days from discovery (for residents of **Colorado** and **Florida**), as analyzed in section 27.08[4]. Where a breach occurs as a result of acquisition of information over a period of time by the same person or entity, the series of events may be treated as a single breach under **Alabama** law<sup>1</sup> (and generally, as a practical matter, in all states, assuming that the intrusions are related).<sup>2</sup>

Under the laws of many states modeled on the first security breach notification law, which was enacted in **California**, the *breach of the security of the system* means “unauthorized acquisition<sup>3</sup> (or in **Maine**, acquisition, release or use)<sup>4</sup> of computerized data” (or in some states such as **New Jersey**, *computerized records*)<sup>5</sup> that compromises<sup>6</sup> the security,

---

telephone number for the Office and the Department in the notice. *Id.*

#### [Section 27.08[3][A]]

<sup>1</sup>See Ala. Code § 8-38-2(1).

<sup>2</sup>See *infra* § 27.08[4].

<sup>3</sup>Some state statutes, such as the ones passed in **Connecticut**, **Kansas**, **Louisiana**, **Missouri** and **Ohio**, impose notification obligations in the event of unauthorized access and acquisition of personal information, rather than merely acquisition. Missouri, however, exempts from this definition “[g]ood faith acquisition of personal information by a person or that person’s employee or agent for a legitimate purpose” provided that the personal information is not used in violation of applicable law or in “a manner that harms or poses an actual threat to the security, confidentiality, or integrity of the personal information.” Mo. Rev. Stat. § 407.1500.1(1).

<sup>4</sup>**Maine** defines *breach of the security of the system or security breach* to mean “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 . . . .” Me. Rev. Stat. Ann. tit. 10, § 1347(1).

<sup>5</sup>See N.J. Stat. Ann. § 56:8-163(b).

<sup>6</sup>**Oregon** defines breach to mean the unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information maintained by the person (or, in

confidentiality, or integrity<sup>7</sup> of personal information<sup>8</sup> maintained by that person or business. **Florida**, in a 2014 amendment, streamlined its definition of “breach” or “breach of security” to mean simply “unauthorized access of data in electronic form containing personal information[,]”<sup>9</sup> which **Alabama** subsequently adopted when it enacted a security breach notification statute in 2018, as applied to “sensitive personally identifying information.”<sup>10</sup>

**Washington**, in 2015, broadened its definition to “unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal information main-

---

**California, the District of Columbia, Minnesota, and the Virgin Islands**, maintained by the person or business). See Cal. Civ. Code § 1798.82(g); D.C. Code § 28-3851(1); Minn. Stat. Ann. § 325E.61(d); Or. Rev. Stat. Ann. § 646A.602(1)(a); V.I. Code Ann. tit. 14, § 2209(d). **Montana, South Carolina and Wyoming** further define breach to mean the unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information maintained by the person or business and causes some harm to a state resident. See Mont. Code Ann. § 30-14-1704(4)(a) (“causes or is reasonably believed to cause loss or injury to a Montana resident.”); Mont. Code Ann. § 2-6-1501(1)(b) (“causes or is reasonably believed to cause loss or injury to a person”); S.C. Code Ann. § 39-1-90(d)(1) (“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.”); Wyo. Stat. Ann. § 40-12-501(a)(i) (“causes or is reasonably believed to cause loss or injury to a resident of this state.”).

<sup>7</sup>**New Hampshire** omits reference to the integrity of the data. See 31 N.H. Rev. Stat. Ann. § 359-C:19(V).

<sup>8</sup>The **Minnesota** provision applicable to state agencies defines a breach of the security of the data to mean “unauthorized acquisition of data maintained by a state agency that compromises the security and classification of the data.” Minn. Stat. Ann. § 13.055(1)(a) (emphasis added). The definition of breach of the security of the system for disclosures by individuals and businesses is consistent with the definition employed by California and a majority of states. See Minn. Stat. Ann. § 325E.61(1)(d).

<sup>9</sup>Fla. Stat. Ann. § 501.171(1)(a). *Data in electronic form* is defined to mean “any data stored electronically or digitally on any computer system or other database and includes recordable tapes and other mass storage devices.” *Id.* § 501.171(1)(d). The definition of *personal information* is set forth in section 501.171(1)(g) and discussed below in section 27.08[3][B].

<sup>10</sup>See Ala. Code § 8-38-2(1) (providing that, subject to exceptions, “[t]he unauthorized acquisition of data in electronic form containing sensitive personally identifying information. Acquisition occurring over a period of time committed by the same entity constitutes one breach.”). *Sensitive personally identifying information* is defined in section 8-38-2(6).

tained by the person or business.”<sup>11</sup> Notably, this definition is no longer limited to *computerized* data. Washington further provides that “[g]ood faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system when the personal information is not used or subject to further unauthorized disclosure.”<sup>12</sup>

Subject to the exceptions and variations noted in this section, security breach notification laws generally compel notice when *unencrypted personal information* in *electronic* form has been compromised (and, in several states, only if computerized data is part of a multi-person database).<sup>13</sup>

Notification statutes typically compel disclosure<sup>14</sup> either based on the risk that a security breach in fact occurred or more narrowly because of the risk of adverse consequences flowing from a breach. Thus, notice may be required under some statutes based on a *potential* breach, whereas it would not be required under others that focus on the potential risk of harm. The terminology actually used in individual statutes, which tend to vary in small but sometimes meaningful respects, may expand or contract notification obligations beyond the grounds suggested by these generalizations.

Disclosure under the **California** statute (and others mod-

---

<sup>11</sup>Wash. Rev. Code Ann. § 19.255.010(4); Wash. Rev. Code Ann. § 42.56.590(4).

<sup>12</sup>Wash. Rev. Code Ann. § 19.255.010(4); Wash. Rev. Code Ann. § 42.56.590(4).

<sup>13</sup>Under the notification statutes in effect in **Kentucky, Oklahoma** (for breaches involving individuals and entities, not government agencies), **Virginia** and **West Virginia**, unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information is only defined as a “breach of the security of a system” if, among other things, the computerized data is “part of a database of personal information regarding multiple individuals . . . .” Ky. Rev. Stat. Ann. § 365.732(1)(a); 24 Okl. Stat. Ann. § 162; Va. Code Ann. § 18.2-186.6(A); W. Va. Code § 46A-2A-101(1). Security breach is similarly limited to information that is part of a database of personal information regarding multiple individuals under **Arizona, Michigan** and **Pennsylvania** law. See Ariz. Code § 18-552; Mich. Comp. Laws Ann. § 445.63(b); 73 Pa. Stat. Ann. § 2302. Thus, in these states, a breach that involves only a single individual or data that was not part of a database of personal information of multiple individuals would not need to be disclosed to state residents.

<sup>14</sup>Notification statutes direct when notice must be provided either directly or based on the scope of exemptions created to otherwise broad obligations to provide notice.

eled on it) is required when unencrypted (or in some cases encrypted<sup>15</sup>) personal information “was, *or is reasonably believed to have been*, acquired by an unauthorized person.”<sup>16</sup> In other words, notice is required even if a breach in fact has not occurred so long as there is a reasonable belief that it may have.

**Alaska** requires notice where a covered person that owns or licenses personal information in any form that includes personal information on a state resident experiences a breach of the security of the information and has a reasonable belief of unauthorized acquisition.

**Indiana**’s statute says this even more explicitly with respect to businesses that maintain but don’t own data.<sup>17</sup> For owners, Indiana imposes disclosure obligations if a *database*

---

<sup>15</sup>Pursuant to an amendment that took effect in 2017, encrypted information is covered when “the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person and the person or business [or agency] that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that personal information readable or useable.” Cal. Civ. Code §§ 1798.29(a), 1798.82(a). *Encryption key* and *security credential* mean “the confidential key or process designed to render the data useable, readable, and decipherable.” *Id.* §§ 1798.29(l), 1798.82(k).

This aspect of California’s law, which has since been adopted in a number of other states, is analyzed in section 27.08[3][C] in connection with encryption and redaction.

<sup>16</sup>Cal. Civ. Code §§ 1798.29(a), 1798.29(b), 1798.82(a), 1798.82(b) (emphasis added). Under **Maine** law, which includes a similar provision but is only applicable to information brokers, an unauthorized person is defined to include anyone who obtained access to personal information by fraud, misrepresentation, subterfuge or similar deceptive practices. *See* Me. Rev. Stat. Ann. tit. 10, § 1347(8). Under **West Virginia** law, notice to an owner or licensee need only be provided “as soon as practicable following discovery, if the personal information was or the entity reasonably believes [it] was accessed and acquired by an unauthorized person.” W. Va. Code § 46A-2A-102(c). **Florida** similarly requires notice by a covered entity if an individual’s personal information was accessed, or the covered entity reasonably believes that it was accessed, as a result of the breach (which as noted earlier, is defined to mean unauthorized access of data in electronic form containing personal information). Fla. Stat. Ann. §§ 501.171(1)(a), 501.171(4)(a). A *covered entity* is “a sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity” or, for certain purposes, a governmental entity, “that acquires, maintains, stores, or uses personal information.” Fla. Stat. Ann. § 501.171(1)(b).

<sup>17</sup>Indiana requires that a person that maintains computerized data but is not the database owner must notify the database owner if that person “discovers that personal information was or may have been

*owner* “knows, should know, or should have known that the unauthorized acquisition constituting the breach has resulted in or could result in identity deception . . . , identity theft, or fraud affecting an Indiana resident.”<sup>18</sup>

**New Hampshire** similarly errs on the side of disclosure. New Hampshire law provides that when a person doing business in the state, who owns or licenses computerized data that includes personal information, it “shall, when it becomes aware of a security breach, promptly determine the likelihood that the information has been or will be misused.”<sup>19</sup> Notice is required if misuse of the information occurred or if a determination cannot be reached.<sup>20</sup>

**Guam**,<sup>21</sup> **Kansas**,<sup>22</sup> **Kentucky**,<sup>23</sup> **Oklahoma** (for breaches involving individuals and entities, not government agencies),<sup>24</sup> **Virginia**<sup>25</sup> and **West Virginia**<sup>26</sup> focus on the risk of misuse, rather than the fact of breach, and impose disclosure obligations where the individual or commercial entity that experienced a breach “reasonably believes [that the breach] has caused or will cause, identity theft” (or in the case of Guam, Kentucky,<sup>27</sup> Oklahoma, Virginia and West Virginia, “identity theft or other fraud”) to a state resident. **Mississippi** similarly narrows California’s language to apply “if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person *for fraudu-*

---

acquired by an unauthorized person” (Ind. Code § 24-4.9-3-2), subject to certain specified exceptions. *See* Ind. Code § 24-4.9-3-3.

<sup>18</sup>Ind. Code § 24-4.9-3-1(a). A *database owner* is defined as a person that owns or licenses computerized data that includes personal information. Ind. Code § 24-4.9-2-3.

<sup>19</sup>31 N.H. Rev. Stat. Ann. § 359-C:20 (I)(a) (emphasis added).

<sup>20</sup>31 N.H. Rev. Stat. Ann. § 359-C:20 (I)(a) (emphasis added).

<sup>21</sup>9 Guam Code Ann. § 48.20(a).

<sup>22</sup>Kan. Stat. Ann. § 50-7a01(h).

<sup>23</sup>Ky. Rev. Stat. Ann. § 365.732(1)(a); *see also* Ky. Rev. Stat. Ann. §§ 61.931(9)(a) (governing breaches involving public agencies and educational institutions).

<sup>24</sup>24 Okl. Stat. Ann. § 162(1).

<sup>25</sup>Va. Code Ann. § 18.2-186.6(A).

<sup>26</sup>W. Va. Code § 46A-2A-101(1).

<sup>27</sup>Kentucky’s statute imposes the obligation to disclose where a breach “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.” Ky. Rev. Stat. Ann. § 365.732(1)(a).

*lent purposes.*”<sup>28</sup> Likewise, disclosure is only required to a person whose personal information “was or is reasonably believed to have been, intentionally acquired by an unauthorized person through a breach of security.”<sup>29</sup>

**Alabama** similarly imposes a disclosure obligation when “sensitive personally identifying information has been acquired or is reasonably believed to have been acquired by an unauthorized person, and is reasonably likely to cause substantial harm to the individuals to whom the information relates . . . .”<sup>30</sup> However, Alabama, which was one of the last states to adopt a security breach notification law, in 2018, also provides more granular detail on how this determination should be made. Alabama law requires that if a covered entity “determines that a breach of security has or may have occurred in relation to sensitive personally identifying information that is accessed, acquired, maintained, stored, utilized, or communicated by, or on behalf of, the covered entity,” it must “conduct a good faith and prompt investigation” that includes all of the following:

- (1) An assessment of the nature and scope of the breach.
- (2) Identification of any sensitive personally identifying information that may have been involved in the breach and the identity of any individuals to whom that information relates.
- (3) A determination of whether the sensitive personally identifying information has been acquired or is reasonably believed to have been acquired by an unauthorized person,<sup>31</sup> and is reasonably likely to cause substantial harm to the individuals to whom the information relates.

---

<sup>28</sup>Miss. Code Ann. § 75-24-29(4) (emphasis added).

<sup>29</sup>Miss. Code Ann. § 75-24-29(2)(b)(iv).

<sup>30</sup>Ala. Code § 8-38-5(a).

<sup>31</sup>The statute also lays out specific circumstances that may be considered “[i]n determining whether sensitive personally identifying information has been acquired or is reasonably believed to have been acquired by an unauthorized person without valid authorization . . . .” Those factors are:

- (1) Indications that the information is in the physical possession and control of a person without valid authorization, such as a lost or stolen computer or other device containing information.
- (2) Indications that the information has been downloaded or copied.
- (3) Indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

- (4) Identification and implementation of measures to restore the security and confidentiality of the systems compromised in the breach.<sup>32</sup>

**South Carolina** compels notice where a breach “compromises the security, confidentiality or integrity of personally identifying information . . . , 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 the consumer.”<sup>33</sup>

**Washington** provides that notice is not required if the breach of the security of the system is not reasonably likely to subject consumers to a risk of harm. On the other hand, a breach 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.<sup>34</sup>

**Wisconsin** provides that notice is not required if there is no material risk of identity theft or fraud.<sup>35</sup> Under **Wyoming’s** statute disclosure is only required if personal information “has been or will be misused.”<sup>36</sup>

**Rhode Island** requires notice of any disclosure of personal information or a “breach of the security of the system which poses a *significant risk* of identity theft to any resident . . . whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person or entity”<sup>37</sup> Notification must be made in the most expedient time possible but no later than forty-five (45) calendar days after confirmation of the breach and the ability to ascertain the information required to fulfill the notice requirements set

---

(4) Whether the information has been made public.

Ala. Code § 8-38-4(b).

<sup>32</sup>Ala. Code § 8-38-4(a).

<sup>33</sup>S.C. Code Ann. §§ 1-11-490(D)(2) (agencies), 39-1-90(D)(1) (persons).

<sup>34</sup>Wash. Rev. Code Ann. § 19.255.010(1); Wash. Rev. Code Ann. § 42.56.590(1)(a).

<sup>35</sup>Wis. Stat. Ann. § 134.98(2)(cm).

<sup>36</sup>Wyo. Stat. Ann. § 40-12-502(a).

<sup>37</sup>R.I. Gen. Laws § 11-49.2-3 (emphasis added); R.I. Gen. Laws § 11-49.3-4(a)(1).

forth in the amended statute.<sup>38</sup> **New Mexico** also adopted a forty-five (45) calendar day outside deadline, but in New Mexico the time period runs from the date of discovery of the breach and New Mexico inverted Rhode Island's "significant risk language" to provide that notwithstanding other provisions of the security breach notification law that would point to an obligation to provide notice, notice is not required if, after an appropriate investigation, a person otherwise required to provide notice "determines that the security breach does not give rise to a significant risk of identity theft or fraud."<sup>39</sup>

**Tennessee** requires that disclosure of a breach be made immediately, but no later than forty-five (45) days from the discovery or notification of the breach, unless a longer time is required due to the legitimate needs of law enforcement.<sup>40</sup>

**Washington** also sets an outside limit of forty-five (45) days from the time 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, additional time is required.<sup>41</sup> This is the same approach adopted by **New Mexico** (except, as previously noted, New Mexico also permits notice to be avoided entirely if the person otherwise required to provide notice determines that the breach does not create a significant risk of identity theft or fraud.<sup>42</sup>

**Delaware** requires that notice be made "without unreasonable delay but not later than 60 days after determination of the breach . . .," except if (1) a shorter time is required by federal law or (2) a law enforcement agency determines that the notice will impede a criminal investigation and has requested that notice be delayed.<sup>43</sup> However, if, through reasonable diligence, it could not have been determined that a

---

<sup>38</sup>R.I. Gen. Laws § 11-49.3-4(a)(2).

<sup>39</sup>N.M. Stat. Ann. §§ 57-12C-6(B), 57-12C-6(C). The 45 day timeline may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation or "as necessary to determine the scope of the security breach and restore the integrity, security and confidentiality of the data system." *Id.* § 57-12C-9.

<sup>40</sup>Tenn. Code Ann. § 47-18-2107(c).

<sup>41</sup>*See* Wash. Rev. Code Ann. § 19.255.010(16); Wash. Rev. Code Ann. § 42.56.590(15).

<sup>42</sup>N.M. Stat. Ann. §§ 57-12C-6(B), 57-12C-6(C), 57-12C-9.

<sup>43</sup>Del. Code Ann. tit. 6, §§ 12B-102(c).

person's information was included in a breach, then notice generally must be sent "as soon as practicable after the determination that the breach of security included the personal information" of such a person.<sup>44</sup>

**South Dakota** requires that notice be provided not later than 60 days from discovery or notification of a breach unless a longer period of time is required due to the legitimate needs of law enforcement as provided under § 22-40-21<sup>45</sup> (in which case the notification must be made not later than 30 days after the law enforcement agency determines that notification will not compromise the criminal investigation).<sup>46</sup>

**Arizona** compels notice where there is "unauthorized acquisitions of and access to unencrypted or unredacted computerized data that *materially compromises the security or confidentiality* of personal information . . ." and "causes or is reasonably likely to cause substantial economic loss to an individual."<sup>47</sup> The **Pennsylvania**<sup>48</sup> security breach statute uses substantially the same language. **Idaho**,<sup>49</sup> **Montana**,<sup>50</sup> **Nevada**,<sup>51</sup> **Oregon**,<sup>52</sup> **Tennessee**,<sup>53</sup> and **Wyoming**,<sup>54</sup> similarly focus on a breach that "materially compromises the security, confidentiality, or integrity" of personal information.

The obligation to provide notice under the **Massachusetts** security breach statute is triggered by "the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and confidential process or key

---

<sup>44</sup>Del. Code Ann. tit. 6, §§ 12B-102(c)(3).

<sup>45</sup>S.D. Codified Laws § 22-40-20.

<sup>46</sup>S.D. Codified Laws § 22-40-21.

<sup>47</sup>Ariz. Rev. Stat. § 18-552(L)(1).

<sup>48</sup>73 Pa. Stat. Ann. § 2302 (requiring notice where there has been "unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of personal information maintained by the entity as part of a database of personal information regarding multiple individuals and that causes or the entity reasonably believes has caused or will cause loss or injury to any resident of this Commonwealth.").

<sup>49</sup>Idaho Code Ann. § 28-51-104(2).

<sup>50</sup>Mont. Code Ann. § 30-14-1704(4)(a); Mont. Code Ann. § 2-6-1501(1)(a).

<sup>51</sup>Nev. Rev. Stat. Ann. § 603A.020.

<sup>52</sup>Or. Rev. Stat. Ann. § 646A.602(1)(a).

<sup>53</sup>Tenn. Code Ann. § 47-18-2107(a)(1)(A).

<sup>54</sup>Wyo. Stat. Ann. § 40-12-501(a)(1).

that is capable of compromising the security, confidentiality, or integrity of personal information . . . that creates a *substantial risk* of identity theft or fraud . . . .”<sup>55</sup>

**Puerto Rico** imposes the obligation to provide notice to customers when the security of a data bank containing all or part of the personal information files of residents has been violated and the file was “not protected by a cryptographic code but only by a password.”<sup>56</sup>

Exceptions exist under some state laws where a breach is unlikely to harm consumers (or create “no reasonable likelihood of financial harm” to consumers in **Iowa** or because misuse “is not reasonably possible” under **New Jersey** or **Vermont**<sup>57</sup> law) or similar standards,<sup>58</sup> subject to the require-

<sup>55</sup>Mass. Gen. L. Ann. ch. 93H, § 1 (emphasis added).

<sup>56</sup>10 L.P.R. Ann. § 4052. Puerto Rico’s statute similarly defines *personal information file* in part to include information that “is legible enough so that in order to access it there is no need to use a special cryptographic code.” *Id.* § 4051(a). A violation

[m]eans any situation in which it is detected that access has been permitted to unauthorized persons or entities to the data files so that the security, confidentiality or integrity of the information in the data bank has been compromised; or when normally authorized persons or entities have had access and it is known or there is a 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 said recordings.

*Id.* § 4051(c).

<sup>57</sup>As amended in 2012, Vermont law provides more detailed statutory guidance on when notice to consumers must be provided. Vt. Stat. Ann. tit. 9, § 2435(b) requires notice of a security breach, which in turn is defined in Vt. Stat. Ann. tit. 9, § 2430(12)(A) to mean “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.” *Id.* § 2430(12)(A) (emphasis added). Thus, notice generally is required if there has been unauthorized access or a reasonable belief of unauthorized access, subject to two major exclusions. First, *security breach* is defined to *exclude* “good faith but unauthorized acquisition of personally identifiable information by an employee or agent of the data collector for a legitimate purpose of the data collector, provided that the personally identifiable information is not used for a purpose unrelated to the data collector’s business or subject to further unauthorized disclosure.” *Id.* § 2430(12)(B). Second, notice to consumers is not required if the data collector “establishes that misuse of personal information is not reasonably possible” (in which case notice to regulators is still required). *See id.* § 2435(d)(1). Further, in determining whether personally identifi-

able information has been acquired or is reasonably believed to have been acquired by a person without valid authorization, the definition of *security breach* states that

a data collector may consider the following factors, among others:

- (i) indications that the information is in the physical possession and control of a person without valid authorization, such as a lost or stolen computer or other device containing information;
- (ii) indications that the information has been downloaded or copied;
- (iii) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported; or
- (iv) that the information has been made public.

*Id.* § 2430(12)(C).

<sup>58</sup>For example, the **Arkansas** and **Louisiana** statutes provide that “notification is not required if, after a reasonable investigation, the person or business determines that there is no reasonable likelihood of harm . . .” to consumers (Arkansas) or state residents (Louisiana). Ark. Code Ann. § 4-110-105(d); La. Stat. § 51:3074(I). **Alaska**’s statute provides the same, except it uses the terminology “not a reasonable likelihood” instead of “no reasonable likelihood.” Alaska Stat. § 45.48.010(c). **Connecticut** similarly exempts a person from notification obligations if “the person reasonably determines that the breach will not likely result in harm to the individuals whose personal information has been acquired and accessed.” Conn. Gen. Stat. Ann. § 36a-701b(b)(1). **Delaware** and **Mississippi** adopted very similar language to Connecticut. *See* Del. Code Ann. tit. 6, § 12B-102(a) (applicable where “the person reasonably determines that the breach of security is unlikely to result in harm to the individuals whose personal information has been breached.”); Miss. Code Ann. § 75-24-29(3) (“Notification shall not be required if, after an appropriate investigation, the person reasonably determines that the breach will not likely result in harm to the affected individuals.”).

**Oregon** provides that notice is not required if, after an appropriate investigation or after consultation with relevant federal, state or local agencies responsible for law enforcement, “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. Ann. § 646A.604(8). This determination, however, must be documented and the documentation must be maintained for five years. *See id.* **South Dakota** includes a similar provision, but only requires retention for three years. *See* S.D. Codified Laws § 22-40-20 (“An information holder is not required to make a disclosure under this section if, following an appropriate investigation and notice to the attorney general, the information holder reasonably determines that the breach will not likely result in harm to the affected person.”). **Maryland** likewise only requires retention for three years. *See* Md. Code Ann., Com. Law § 14-3504(b)(4). **Iowa** provides that 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.”

ments that this decision be documented and retained for

---

Iowa Code Ann. § 715C.2(6). Any such determination must be documented in writing and maintained for five years. *Id.* **Missouri's** security breach law contains a similar provision, but provides that notice is not required if the person determines that a "risk of identity theft or other fraud to any consumer is not reasonably likely to occur as a result of the breach." Mo. Rev. Stat. § 407.1500.2(5).

**Florida** likewise excuses a person from providing notice if, after "an appropriate investigation and consultation with relevant federal, state, or local law enforcement agencies, the covered entity reasonably determines that the breach has not and will not likely result in identity theft or any other financial harm to the individuals whose personal information has been accessed." Fla. Stat. Ann. § 501.171(4)(c). Such a determination must be documented in writing, provided to the Department of Legal Affairs within thirty days of the determination, and the records supporting the determination must be maintained for at least five years. *Id.*

As noted in the text, with respect to determinations that notice need not be sent, documentation must be retained for three years under **Maryland** and **South Dakota** law and for five years in **Alabama, Alaska, Florida, Iowa, Louisiana, Missouri, New Jersey** and **Oregon**. In addition, notice of a determination that notice to consumers is not required must be provided to state officials in **Alaska, Florida, South Dakota, and Vermont** (or if requested, within 30 days of the request, for residents of **Louisiana**). Notice to state agencies is separately addressed in section 27.08[8].

**Michigan** requires notice "[u]nless the person or agency determines that the security breach has not or is not likely to cause substantial loss or injury to, or result in identity theft with respect to, one or more residents of the state . . . ." Mich. Comp. Laws Ann. § 445.72(1). In determining whether a security breach is not likely to cause substantial loss or injury to, or result in identity theft with respect to, one or more Michigan residents, a person or agency must "act with the care that an ordinarily prudent person or agency in like position would exercise under the circumstances." Mich. Comp. Laws Ann. § 335.72(3).

**Washington's** law provides that notice is not required if the breach of the security of the system is not reasonably likely to subject consumers to a risk of harm. On the other hand, 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 Ann. § 19.255.010(1); Wash. Rev. Code Ann. § 42.56.590(1)(a).

**Wisconsin** provides that an entity is not required to provide notice if "[t]he acquisition of personal information does not create a material risk of identity theft or fraud to the subject of the personal information" or if the information "was acquired in good faith by an employee or agent of the entity, if the personal information is used for a lawful purpose of the entity." Wis. Stat. Ann. § 134.98(2)(cm).

By contrast, **New Jersey** provides that notice is not required if a business or public entity "establishes that misuse of the information is not

three years in **Maryland**<sup>59</sup> and **South Dakota**,<sup>60</sup> and five years in **Alabama**,<sup>61</sup> **Alaska**,<sup>62</sup> **Florida**,<sup>63</sup> **Iowa**,<sup>64</sup> **Louisiana**,<sup>65</sup> **Missouri**,<sup>66</sup> **New Jersey**<sup>67</sup> and **Oregon**,<sup>68</sup> and the further requirement to provide notice of such a determination to state officials in **Alaska**,<sup>69</sup> **Florida**,<sup>70</sup> **South Dakota**,<sup>71</sup> and **Vermont**<sup>72</sup> (or if requested, within 30 days of the request, for residents of **Louisiana**<sup>73</sup>). Notice to state agencies is separately addressed in section 27.08[8].

In evaluating under **New York** law “in the most expedi-

---

reasonably possible” which is a somewhat tougher standard. *See* N.J. Stat. Ann. § 56:8-163(a) (emphasis added).

As discussed in the text following this footnote, Alabama, Alaska, Florida, Iowa, Missouri, Louisiana, New Jersey, and Oregon security breach notification laws all require that if a determination is made that notice is not required, the determination must be made in writing and maintained for five years, while Maryland and South Dakota require that the determination be retained for at least three years.

<sup>59</sup>Md. Code Ann., Com. Law § 14-3504(b)(4). A *record* is defined under Maryland law as “information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.” *Id.* § 14-3501(f).

<sup>60</sup>S.D. Codified Laws § 22-40-20.

<sup>61</sup>Ala. Code § 8-38-5(f).

<sup>62</sup>Alaska Stat. § 45.48.010(c).

<sup>63</sup>Fla. Stat. Ann. § 501.171(4)(c).

<sup>64</sup>Iowa Code Ann. § 715C.2(6).

<sup>65</sup>La. Rev. Stat. Ann. § 51:3074(I).

<sup>66</sup>Mo. Rev. Stat. § 407.1500.2(5).

<sup>67</sup>N.J. Stat. Ann. § 56:8-163(a).

<sup>68</sup>Ore. Stat. § 646A.604(8).

<sup>69</sup>Alaska Stat. § 45.48.010(c).

<sup>70</sup>Fla. Stat. Ann. § 501.171(4)(c).

<sup>71</sup>S.D. Codified Laws § 22-40-20.

<sup>72</sup>Like New Jersey, Vermont provides that notice is not required if a data collector “establishes” that “misuse of personal information is not reasonably possible” but under Vermont law notice of this determination must be sent with “a detailed explanation” to the Vermont attorney general or the department of banking, insurance, securities and health care administration. Vt. Stat. Ann. tit. 9, § 2435(d)(1). The notice may be designated as a trade secret and treated confidentially if applicable. *See id.* If a data collector subsequently determines that misuse in fact has occurred or is occurring, however, it must provide notice to consumers as otherwise required by Vermont law. *Id.* § 2435(d)(2).

<sup>73</sup>La. Rev. Stat. Ann. § 51:3074(I).

ent time possible and without unreasonable delay”<sup>74</sup> whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization, a business “may consider the following factors, among others”:

- indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information;
- indications that the information has been downloaded or copied; or
- indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.<sup>75</sup>

Virtually every state security breach statute carves out employee access. Statutes generally provide that good faith acquisition (or, in **Maine**,<sup>76</sup> acquisition, release or use, or for government entities in **Minnesota**, acquisition or access to government data, which encompasses data that is merely viewable<sup>77</sup>) of personal information by an employee or agent of the person or business (or in Illinois, the data collector, or **Alabama**, a “covered entity”) for the purposes of the person or business (or, in **Illinois**, **New Jersey** and **New Mexico**, “a legitimate business purpose,” in **Nevada**, “a legitimate purpose of the data collector . . .,” under the law of **Guam**, lawful purpose, or according to **Ohio** law, not “an unlawful purpose or subject to further unauthorized disclosure”) is exempted, provided the personal information is not used or subject to further (or unauthorized) disclosure.<sup>78</sup> **Colorado**,<sup>79</sup>

<sup>74</sup>N.Y. Gen. Bus. L. § 899-aa(2).

<sup>75</sup>N.Y. Gen. Bus. L. § 899-aa(1)(c).

<sup>76</sup>Me. Rev. Stat. Ann. tit. 10, § 1347(1).

<sup>77</sup>See Minn. Stat. Ann. §§ 13.055(1)(a), 13.055(1)(c).

<sup>78</sup>See, e.g., Alaska Stat. § 45.48.050; Ariz. Rev. Stat. Ann. § 18-552(L)(1); Ark. Code Ann. § 4-110-103(1)(B); Cal. Civ. Code § 1798.29(f) (agencies); Cal. Civ. Code § 1798.82(g); Colo. Rev. Stat. Ann. § 6-1-716(1)(h) (for covered entities); D.C. Code § 28-3851(1); 9 Guam Code Ann. § 48.20(a); Haw. Rev. Stat. Ann. § 487N-1; 815 Ill. Comp. Stat. Ann. 530/5; Ind. Code Ann. § 24-4.9-2-2(b)(1); Ky. Rev. Stat. Ann. § 365.732(1)(a); La. Rev. Stat. Ann. § 51:3073(2); Md. Code Ann., Com. Law § 14-3504(a)(2); Md. Code Ann., State Gov’t § 10-1305(a)(2); Mont. Code Ann. § 30-14-1704(4)(a); Neb. Rev. Stat. § 87-802(1); Nev. Rev. Stat. Ann. § 603A.020; N.H. Rev. Stat. Ann. § 359-C:19(V); N.J. Stat. Ann. § 56:8-161;

**Delaware**,<sup>80</sup> **Kansas**,<sup>81</sup> **Maine**,<sup>82</sup> **Rhode Island**,<sup>83</sup> **South Dakota**,<sup>84</sup> **Tennessee**,<sup>85</sup> (**Texas**<sup>86</sup> and **Alabama**<sup>87</sup>, albeit phrased slightly differently, involving sensitive PII), the **U.S. Virgin Islands**,<sup>88</sup> **Washington**,<sup>89</sup> and **Wyoming**<sup>90</sup> exclude good faith acquisition by an agent or employee (and in the case of Maine, provide that release and use 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.”). **Idaho**<sup>91</sup> law is the same, except it applies to an employee or agent of an individual,

N.M. Stat. Ann. § 57-12C-2(D); N.Y. Gen. Bus. Law § 899-aa(1)(c); N.Y. State Tech. Law § 208(1)(b); N.C. Gen. Stat. Ann. § 75-61(14); Ohio Rev. Code Ann. § 1347.12(A)(2)(b)(i); Ohio Rev. Code Ann. § 1349.19(A)(1)(b)(i); Okla. Stat. Ann. tit. 24, § 162(1); Okla. Stat. Ann. tit. 74, § 3113.1(D)(1); 73 Pa. Stat. Ann. § 2302; S.C. Code Ann. § 37-20-110(15); S.C. Code Ann. § 39-1-90(D)(1); S.C. Code Ann. § 1-11-490(D)(2); Vt. Stat. Ann. tit. 9, § 2430(12)(B); Va. Code Ann. § 18.2-186.6(a); Va. Code Ann. § 32.1-127.1:05(A) (medical information); W. Va. Code Ann. § 46A-2A-101(1).

<sup>79</sup>Colo. Rev. Stat. Ann. § 6-1-716 (1)(h) (“Good faith acquisition of personal information by an employee or agent of a covered entity for the covered entity’s business purposes is not a security breach if the personal information is not used for a purpose unrelated to the lawful operation of the business or is not subject to further unauthorized disclosure.”).

<sup>80</sup>Del. Code Ann. tit. 6, § 12B-101(1).

<sup>81</sup>Kan. Stat. Ann. § 50-7a01(h).

<sup>82</sup>Me. Rev. Stat. Ann. tit. 10, § 1347 (1).

<sup>83</sup>R.I. Gen. Laws § 11-49.3-3(a)(1).

<sup>84</sup>S.D. Codified Laws § 22-40-19.

<sup>85</sup>Tenn. Code Ann. § 47-18-2107(a)(1)(B).

<sup>86</sup>Tex. Bus. & Com. Code Ann. § 521.053(a) (“Good faith acquisition of sensitive personal information by an employee or agent of the person for the purposes of the person is not a breach of system security unless the person uses or discloses the sensitive personal information in an unauthorized manner.”).

<sup>87</sup>Ala. Code § 8-38-2(1)(a) (“Good faith acquisition of sensitive personally identifying information by an employee or agent of a covered entity, unless the information is used for a purpose unrelated to the business or subject to further unauthorized use.”).

<sup>88</sup>V.I. Code Ann. tit. 14, §§ 2208(d), 2209(d).

<sup>89</sup>Wash. Rev. Code Ann. §§ 19.255.010(4), 42.56.590(4).

<sup>90</sup>Wyo. Stat. Ann. § 40-12-501(a)(i).

<sup>91</sup>Idaho Code Ann. § 28-51-104(2).

business or government agency. **Georgia**<sup>92</sup> law also tracks Colorado and Delaware, except it applies to an employee or agent of an information broker or data collector. **Indiana**<sup>93</sup> law is substantially the same, for employees of government agencies.

**Florida**<sup>94</sup> excludes good faith access of personal information by an employee or agent, provided that the information is not used for a purpose unrelated to the business or subject to further unauthorized use, which carves out improper access by employees or agents, even if not further disclosed by them. **Iowa**<sup>95</sup> and **Missouri**<sup>96</sup> include the standard exception, but instead of the proviso that the information only be used in a business and/or not unlawfully, their statutes provide that the use not be “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.” **Michigan**<sup>97</sup> similarly contains the variation that good faith employee access not involve “misuse [of] any personal information or disclos[ur]e [of] any personal information to an unauthorized person.” **Wisconsin** simply provides that notice is not required if “personal information was acquired in good faith by an employee or agent of the entity, if the personal information is used for a lawful purpose of the entity.”<sup>98</sup>

With respect to employees, **Tennessee**, in addition to excluding acquisition by an employee or agent for the purposes of the information holder (if the information is not used or subject to further unauthorized disclosure),<sup>99</sup> defines *breach* to mean acquisition by an *unauthorized person*,<sup>100</sup> which in turn is defined to *include* “an employee of the information holder who is discovered by the information holder to have obtained personal information with the intent to use it

---

<sup>92</sup>Ga. Code Ann. § 10-1-911(1).

<sup>93</sup>Ind. Code § 4-1-11-2(b)(1).

<sup>94</sup>Fla. Stat. Ann. § 501.171(1)(a).

<sup>95</sup>Iowa Code Ann. § 715C.1(1).

<sup>96</sup>Mo. Ann. Stat. § 407.1500(1).

<sup>97</sup>Mich. Comp. Laws Ann. § 445.63(b)(iii).

<sup>98</sup>Wis. Stat. Ann. § 134.98(2)(cm)(2).

<sup>99</sup>Tenn. Code Ann. § 47-18-2107(a)(1)(B).

<sup>100</sup>Tenn. Code Ann. § 47-18-2107(a)(1)(A).

for an unlawful purpose.”<sup>101</sup>

**Nebraska**<sup>102</sup> and **Ohio**<sup>103</sup> further expressly exempt the 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.

### 27.08[3][B] Data Elements That Give Rise To A Disclosure Obligation—Defining Personal Information

*Personal information* (also known as *private information* under **New York** law,<sup>1</sup> *sensitive personal information* under **Texas** law,<sup>2</sup> *sensitive personally identifiable information* under **Alabama** law,<sup>3</sup> or *personally identifiable information*

<sup>101</sup>Tenn. Code Ann. § 47-18-2107(a)(5).

<sup>102</sup>Neb. Rev. Stat. § 87-802(1).

<sup>103</sup>Ohio Rev. Code Ann. § 1349.19(A)(1)(b)(ii).

#### [Section 27.08[3][B]]

<sup>1</sup>McKinney’s Gen. Bus. L. § 899-aa(b).

<sup>2</sup>See Tex. Bus. & Comm. Code § 521.002; Tex. Gov’t Code §§ 205.010, 2054.1125. In addition to data elements typically included in most statutes (first name or initial and last name plus Social Security number, driver’s license or government ID or account number or credit or debit card in combination with any requested security code, access code, or password that would permit access to an individual’s financial account), *sensitive personal information* is information that identifies an individual and relates to (i) the physical or mental health or condition of the individual, (ii) the provision of health care to the individual, or (iii) payment for the provision of health care to the individual. *Id.* § 521.002 (a)(2)(B).

<sup>3</sup>Ala. Code § 8-38-2(6). Subject to exclusions, *sensitive personally identifying information* is defined to include:

1. A non-truncated Social Security number or tax identification number.
2. A non-truncated driver’s license number, state-issued identification card number, passport number, military identification number, or other unique identification number issued on a government document used to verify the identity of a specific individual.
3. A financial account number, including a bank account number, credit card number, or debit card number, in combination with any security code, access code, password, expiration date, or PIN, that is necessary to access the financial account or to conduct a transaction that will credit or debit the financial account.
4. Any information regarding an individual’s medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

under **Kentucky**<sup>4</sup> and **Vermont** law<sup>5</sup>) generally is defined to include an individual's first name or first initial and last name (or under **D.C.** law a first name or first initial and last name or a phone number or an address) in combination with ("and linked to" under the statutes enacted in **Guam, Ohio, Oklahoma, Pennsylvania, South Carolina, Virginia** and **Wisconsin**) any one or more of the following data elements, when either the name or the data elements are not encrypted<sup>6</sup> (or where applicable, encrypted or redacted or rendered unusable): Social Security number; driver's license

5. An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual.
6. A user name or email address, in combination with a password or security question and answer that would permit access to an online account affiliated with the covered entity that is reasonably likely to contain or is used to obtain sensitive personally identifying information.

*Id.* § 8-38-2(6)(a).

<sup>4</sup>Ky. Rev. Stat. Ann. § 365.732(1)(c).

<sup>5</sup>Vt. Stat. Ann. tit. 9, § 2430(9)(A).

<sup>6</sup>A number of states use the **California** formulation "when either the name or the data elements are not encrypted." Read literally, this language would mandate notification any time a person's name appeared in unencrypted form together with encrypted data elements, even though by definition the encrypted elements could not easily be deciphered and used for identity theft or fraud. States that use this formulation include **Arkansas, Delaware, Georgia, Idaho, Illinois, Maine** (modified to refer to encryption or redaction), **Minnesota, Montana, Oklahoma** (for breaches involving state agencies, but not individuals or entities), **Tennessee, Vermont** (modified to refer to encrypted or redacted or protected by another method that renders the data elements unreadable or unusable by unauthorized persons) and **Washington**, among others.

A better formulation, found in later-enacted statutes, defines *identifying information* and *data elements* to constitute personal information "when the data elements are neither encrypted nor redacted." *E.g.*, Kan. Stat. Ann. § 50-7a01(g); Okla. Stat. Ann. tit. 24, § 162(6) (for breaches involving individuals or entities); *see also, e.g.*, Fla. Stat. Ann. § 501.171(1)(g)(2) (excluding from the definition of *personal information* "information that is encrypted, secured, or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable."); Ohio Rev. Code Ann. § 1347.12(b)(6)(A) ("when the data elements are not encrypted, redacted, or altered by any method or technology in such a manner that the data elements are unreadable."); Ohio Rev. Code Ann. § 1349.13(A)(7)(a); Or. Rev. Stat. Ann. § 646A.602(11) (defining *personal information*, in part, "if encryption, redaction or other methods have not rendered the data elements unusable . . ."); 73 Pa. Stat. Ann. § 2303 ("when the data elements are not encrypted or redacted"); Wis. Stat. Ann.

or state Identification Card number (or in **Puerto Rico** voter's identification card or other official identification, **Missouri**, driver's license number "or other unique identification number created or collected by a government body[,] in **Florida** "passport number, military identification number, or other similar number issued on a government document used to verify identity"<sup>7</sup> or in **Colorado**, "Student, Military, or Passport identification number; Driver's license number or Identification card number"<sup>8</sup>) and/or account number, (expiration date, in **Indiana**<sup>9</sup> and **Iowa**<sup>10</sup>) credit or debit card number (and in the case of **Iowa** and **Nebraska**, unique

---

§ 134.98(1)(b) ("if the element is not publicly available information and is not encrypted, redacted, or altered in a manner that renders the element unreadable"). These state statutes (other than Florida and Oregon) also use the "linked to" terminology referenced above in the text. Some states such as **Mississippi** simply omit this additional clause. See Miss. Code Ann. § 75-24-29(2)(b).

**Illinois**, effective January 1, 2017, changed the standard term "when either the name or the data elements are not encrypted or redacted" to include, alternatively, where either the name or the data elements "are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the name or data elements have been acquired without authorization through the breach of security . . . ." 815 Ill. Comp. Stat. Ann. § 530/5(1).

**Oregon** has separate definitions for *personal information* depending on whether a person's first name or initial and last name have been exposed. Like most other statutes, it defines personal information to include a person's first name or initial and last name in combination with certain data elements. See Or. Rev. Stat. Ann. § 646A.602(11)(a). Oregon also defines personal information as just a single data element (driver's license, passport, financial account, physical characteristics, health insurance policy, medical history) *if* encryption, redaction or other methods have not rendered the data element unusable *and* the data element (or combination of data elements) would enable a person to commit identity theft against a consumer. Or. Rev. Stat. Ann. § 646A.602(11)(a)(B).

<sup>7</sup>Fla. Stat. Ann. § 501.171(1)(g)(1)(II). Passport numbers are also included in the security breach notification laws in effect in **Colorado**, **Connecticut**, **Michigan**, **North Carolina** and **Oregon**. Other state security breach notification laws (including Connecticut, Florida, Michigan, North Carolina and **North Dakota**) apply to employer IDs, which presumably would include military IDs. Still others, such as **Oregon**, apply to IDs issued by the United States, which also presumably would include military IDs. **Alabama** more broadly includes any "unique identification number issued on a government document used to verify the identity of a specific individual." Ala. Code § 8-38-2(6)(a)(1).

<sup>8</sup>Colo. Rev. Stat. Ann. §§ 6-1-716(1)(g)(I)(A), 24-73-103(g)(I)(A).

<sup>9</sup>Ind. Code § 24-4.92-2-10(D).

<sup>10</sup>Iowa Code Ann. § 715C.1(11)(a)(3).

electronic identification numbers or routing codes)<sup>11</sup> alone<sup>12</sup> or in combination with any required security code, access

<sup>11</sup>Iowa Code Ann. § 715C.1(11)(a)(4); Neb. Rev. Stat. § 87-802(5)(iv).

<sup>12</sup>See Wis. Stat. Ann. § 134.98(1)(b)(3) (“financial account number, including a credit or debit card account number, or any security code, access code, or password that would permit access to the individual’s financial account.”); Haw. Rev. Stat. Ann. § 487N-1 (“[a]ccount number, credit or debit card number, access code, or password that would permit access to an individual’s financial account.”); Mass. Gen. L. Ann. ch. 93H, § 1 (“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 . . .”).

Under **Georgia** and **Maine** law, personal information includes an “[a]ccount 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 . . .” Ga. Code Ann. § 10-1-911(6)(C); Me. Rev. Stat. Ann. tit. 10, § 1347(6)(C). Passwords, PINs or other access codes are separately included as personal information under the Georgia statute. Ga. Code Ann. § 10-1-911(6)(D); Me. Rev. Stat. Ann. tit. 10, § 1347(6)(D). Vermont also adopts this approach, using very similar but not identical language. See Vt. Stat. Ann. tit. 9, § 2430(9)(A)(iii). These and other elements of personal information need not be found in combination with a person’s first name or first initial and last name to trigger a notification obligation under Georgia law “if the information compromised would be sufficient to perform or attempt to perform identity theft against the person whose information was compromised.” Ga. Code Ann. § 10-1-911(6)(E). Maine law includes a substantially identical provision. See Me. Rev. Stat. Ann. tit. 10, § 1347(6)(E).

**Illinois** law largely follows California law in its definition of *personal information*, as noted later in this section, but previously defined it as a person’s first name or first initial and last name when combined with an account number or credit or debit card number or an account number or credit number in combination with “any required security code, access code, or password that would permit access to an individual’s financial account.” 815 Ill. Comp. Stat. Ann. 530/5 (emphasis added). **West Virginia** follows the old Illinois formulation, similarly defining the data element as a “[f]inancial account number, or credit card, or debit card number in combination with any required security code or password that would permit access to a resident’s financial accounts.” W. Va. Code § 46A-2A-101(6). **Iowa** employs the same definition as West Virginia except it substitutes the word “individual” for “resident.” Iowa Code Ann. § 715C.1(11)(a)(3).

The **District of Columbia** statute (after specifically enumerating a social security number, driver’s license or D.C. Identification Card number and credit or debit card number) refers more generally to “[a]ny other number or code or combination of numbers or codes, such as account number, security code, access code, or password, that allows access to or use of an individual’s financial or credit account.” D.C. Code § 28-3851(3)(A)(ii).

code, or password (or, in **South Dakota**,<sup>13</sup> additionally a routing number, PIN, or any additional information) that would permit access to an individual's financial account.<sup>14</sup> **North Carolina** and **South Carolina** also include "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 and individual."<sup>15</sup>

**Montana**,<sup>16</sup> **Rhode Island**,<sup>17</sup> and **Wyoming**<sup>18</sup> further include a tribal identification card.

At least ten states expressly require notification of security breaches involving biometric data. **Colorado**,<sup>19</sup> **Connecticut** (but only for state contractors),<sup>20</sup> **Delaware**,<sup>21</sup> **Illi-**

<sup>13</sup>S.D. Codified Laws § 22-40-19(4)(c).

<sup>14</sup>*See, e.g.*, Alaska Stat. § 45.48.090(7); Cal. Civ. Code §§ 1798.29(g)(1) (state agencies), 1798.82(h)(1) (persons and businesses); Del. Code Ann. tit. 6, § 12B-101(4)(a)(3); Fla. Stat. Ann. § 501.171(1)(g)(1)(III) (using the language "necessary to permit access to an individual's financial account."); 9 Guam Code Ann. § 48.20(f)(3); Kan. Stat. Ann. § 50-7a01(g)(3); Ky. Rev. Stat. Ann. § 365.732(1)(c)(3); La. Stat. Ann. § 51:3073(4)(b); Md. Code Ann., Com. Law § 14-3501(e)(1)(i)(3) (an "account number, a credit card number, or a debit card number, in combination with any required security code, access code, or password, that permits access to an individual's financial account"); Minn. Stat. Ann. § 325E.61(1)(e); Miss. Code Ann. § 75-24-29(2)(b); Mo. Rev. Stat. § 407.1500.1(9); Mont. Code Ann. § 30-14-1704(4)(b)(i)(C); Mont. Code Ann. § 2-6-1501(4)(a) (as applicable to state agencies); 31 N.H. Rev. Stat. Ann. § 359-C:19(IV)(a); R.I. Gen. Laws § 11-49.2-5(c)(3); S.C. Code Ann. § 39-1-90(D)(3)(c); Tenn. Code Ann. § 47-18-2107(a)(4)(iii); Va. Code Ann. § 18.2-186.6(A) (individuals and entities); V.I. Code Ann. tit. 14, §§ 2208(e) (agencies), 2209(e) (persons and businesses); Wash. Code Ann. §§ 19.255.010(5)(c) ("Full account number, credit or debit card number, or any required security code, access code, or password that would permit access to an individual's financial account."); persons and businesses), 42.56.590(5)(c) (state agencies).

<sup>15</sup>N.C. Gen. Stat. Ann. § 14-113.20; S.C. Code Ann. § 39-1-90(D)(3)(d).

<sup>16</sup>Mont. Code Ann. § 30-14-1704(4)(b)(i)(C); Mont. Code Ann. § 2-6-1501(4)(a)(ii).

<sup>17</sup>R.I. Gen. Laws § 11-49.3-3(a)(8)(ii).

<sup>18</sup>Wyo. Stat. Ann. §§ 6-3-901(b)(vi), 40-12-501(a)(vii).

<sup>19</sup>Colo. Rev. Stat. Ann. §§ 6-1-716(1)(a), 6-1-716(1)(g)(I)(A), 24-73-103(g)(I)(A).

<sup>20</sup>Conn. Gen. Stat. Ann. § 4e-7015(a)(4).

<sup>21</sup>Del. Code Ann. tit. 6, § 12B-101(4)(a)(8) ("[u]nique biometric data generated from measurements or analysis of human body characteristics for authentication purposes").

nois,<sup>22</sup> Iowa,<sup>23</sup> Louisiana,<sup>24</sup> Maryland,<sup>25</sup> Nebraska,<sup>26</sup> New Mexico,<sup>27</sup> Texas,<sup>28</sup> Wisconsin<sup>29</sup> and Wyoming<sup>30</sup> add to this list of personally identifying information unique biometric data, such as a fingerprint, voice print (referenced in the Maryland, Nebraska, New Mexico and Wisconsin statutes), retina or iris image, or other unique physical representation (or, in the case of Iowa, digital representation of biometric data). Wisconsin also includes an individual's deoxyribonucleic acid profile.<sup>31</sup> New Mexico adds facial characteristics or hand geometry, all qualified to apply when "used to uniquely and durably authenticate an individual's identity when the individual accesses a physical location, device, system or account . . . ."<sup>32</sup> North Carolina includes a person's digital signature, biometric data, finger prints or checking account.<sup>33</sup> Colorado, in revisions that took effect in late 2018, more expansively includes "unique biometric data generated from measurements or analysis of human body characteristics for the purpose of authenticating the individual when he or she accesses an online account."<sup>34</sup>

North Dakota adds an individual's date of birth, mother's maiden name, medical information, health insurance information, identification number assigned by an employer (in

---

<sup>22</sup>815 Ill. Comp. Stat. Ann. 530/5(1)(F) ("Unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee to authenticate an individual, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data.").

<sup>23</sup>Iowa Code Ann. § 715C.1(11)(a)(5).

<sup>24</sup>La. Rev. Stat. Ann. § 51:3073(4)(a)(v). *Biometric data* means "data generated by automatic measurements of an individual's biological characteristics, such as fingerprints, voice print, eye retina or iris, or other unique biological characteristic that is used by the owner or licensee to uniquely authenticate an individual's identity when the individual accesses a system or account." *Id.*

<sup>25</sup>Md. Code Ann., Com. Law § 14-3501(e)(1)(i)(6).

<sup>26</sup>Neb. Rev. Stat. § 87-802(5)(v).

<sup>27</sup>N.M. Stat. Ann. §§ 57-12C-2(C)(1)(e), 57-12C-6(A).

<sup>28</sup>Tex. Bus. & Com. Code Ann. § 521.002.

<sup>29</sup>Wis. Stat. Ann. § 134.98(1)(b)(5).

<sup>30</sup>Wyo. Stat. Ann. §§ 6-3-901(b)(xiii), 40-12-501(a)(vii).

<sup>31</sup>Wis. Stat. Ann. § 134.98(1)(b)(4).

<sup>32</sup>N.M. Stat. Ann. § 57-12C-2(A).

<sup>33</sup>N.C. Gen. Stat. Ann. §§ 75-61(10), 114-113.20(b).

<sup>34</sup>Colo. Rev. Stat. Ann. § 6-1-716(1)(a).

combination with any required security code, access code, or password), the operator's license number assigned to an individual by the department of transportation, a nondriver color photo ID card assigned to the individual by the department of transportation, or an individual's digitized or electronic signature.<sup>35</sup> When there has been a breach of the security of these data elements—many of which are commonly used for enhanced security to allow access to financial or other accounts—disclosure may be required to affected residents in North Dakota if the breach also included a person's first name or initial and last name (and the data was not encrypted).

**South Dakota**, like North Dakota, includes an identification number assigned by an employer, in combination with any required security code, access code, or password, but also adds in combination with “biometric data generated from measurements or analysis of human body characteristics for authentication purposes . . . .”<sup>36</sup>

**Alabama**,<sup>37</sup> **Connecticut**,<sup>38</sup> **Delaware**,<sup>39</sup> **Florida**,<sup>40</sup> **Maryland**,<sup>41</sup> **Michigan**,<sup>42</sup> **Montana**,<sup>43</sup> **North Carolina**<sup>44</sup> and **Wyoming**<sup>45</sup> include an Individual Taxpayer Identification Number. **Puerto Rico** also lists tax information and work-related evaluations among the data elements that could trigger notification obligations.<sup>46</sup>

State notification laws enumerate data elements covered by the statute. **Maryland**, however, also expressly excludes

<sup>35</sup>N.D. Cent. Code § 51-30-01(4)(a).

<sup>36</sup>S.D. Codified Laws § 22-40-19(4)(e).

<sup>37</sup>Ala. Code § 8-38-2(6)(a)(6).

<sup>38</sup>Conn. Gen. Stat. Ann. § 15-142(4).

<sup>39</sup>Del. Code Ann. tit. 6, § 12B-101(4)(a)(9).

<sup>40</sup>Fla. Stat. Ann. § 817.5685(1).

<sup>41</sup>Md. Code Ann., Com. Law § 14-3501(e)(1)(i)(1).

<sup>42</sup>Mich. Comp. Laws Ann. § 445.63.

<sup>43</sup>Mont. Code Ann. § 30-14-1704(b); Mont. Code Ann. § 33-19-321(6)(b)(E); Mont. Code Ann. § 2-6-1501(4)(a)(v). Montana added this data element, along with an identity protection personal identification number issued by the IRS and medical record information effective in 2015.

<sup>44</sup>N.C. Gen. Stat. Ann. § 14-113.20; N.C. Gen. Stat. Ann. § 75-66.

<sup>45</sup>Wyo. Stat. Ann. §§ 6-3-901(b)(xiv), 40-12-501(a)(vii).

<sup>46</sup>See 10 L.P.R. Ann. § 4051(a).

from the definition of *personal information* a voter registration number.<sup>47</sup>

A breach that results in disclosure of a person's name and email address, without more, generally does not require notification. **North Carolina**, however, may require disclosure if the data could provide access to a financial account or resources. Specifically, the North Carolina statute provides that "personal information" for purposes of assessing notification obligations upon breach, "shall not include electronic identification numbers, electronic mail names or addresses, Internet account numbers, Internet identification names, parent's legal surname prior to marriage, or a password unless this information would permit access to a person's financial account or resources."<sup>48</sup> Thus, where this information would permit access, notification will be required.

**Alabama** provides expressly that a user name or email address constitutes *sensitive personally identifying information* if it is disclosed "in combination with a password or security question and answer that would permit access to an online account affiliated with the covered entity that is reasonably likely to contain or is used to obtain sensitive personally identifying information."<sup>49</sup>

Likewise, disclosure would be required under the **Puerto Rico** statute, where the "names of users and passwords or access codes to public or private information systems" were disclosed in addition to a person's first name or initial and last name.<sup>50</sup>

**Louisiana** adds to the basic list, among other things, a passport number.<sup>51</sup> **Oregon** includes a passport number or other identification number issued by the United States.<sup>52</sup> **Maryland** adds "a passport number, or other identification

---

<sup>47</sup>Md. Code Ann State Gov. § 10-1301(c)(2).

<sup>48</sup>N.C. Gen. Stat. Ann. § 75-65(a); *see also* N.C. Gen. Stat. Ann. §§ 14-113.20(b)(8), 75-61(10) (providing that a name and email address otherwise could trigger a notification obligation).

<sup>49</sup>Ala. Code § 8-38-2(6)(a)(1).

<sup>50</sup>P.R. Laws Ann. tit. 10, § 4051(a)(4).

<sup>51</sup>La. Rev. Stat. Ann. § 51:3073(4)(a)(iv).

<sup>52</sup>Or. Rev. Stat. Ann. § 646A.602(11)(a)(A)(iii).

number issued by the federal government . . . .”<sup>53</sup> **Florida**, as previously noted, likewise includes “passport number, military identification number, or other similar number issued on a government document used to verify identity.”<sup>54</sup> **Delaware** adds a passport number<sup>55</sup> and a state or federal identification card number.<sup>56</sup>

**Oregon** added, effective 2018, a catch-all category—“any other information or combination of information that a person reasonably knows or should know would permit access to the consumer’s financial account . . . .”<sup>57</sup> Oregon also defines personal information to mean any of the data elements or any combination of data elements enumerated in the statute “when not combined with the consumer’s first name or first initial and last name if: (i) Encryption, redaction or other methods have not rendered the data element or combination of data elements unusable; and (ii) The data element or combination of data elements would enable a person to commit identity theft against a consumer.”<sup>58</sup>

**Iowa**, however, limits notification obligations to “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 was subject to a breach . . . .”<sup>59</sup> Notice also need not be provided under Iowa’s statute if there was “no reasonable likelihood of financial harm to the consumers whose personal information

<sup>53</sup>Md. Code Ann., Com. Law § 14-3501(e)(1)(i)(1).

<sup>54</sup>Fla. Stat. Ann. § 501.171(1)(g)(1)(II).

<sup>55</sup>Del. Code Ann. tit. 6, § 12B-101(4)(a)(4).

<sup>56</sup>Del. Code Ann. tit. 6, § 12B-101(4)(a)(2).

<sup>57</sup>Or. Rev. Stat. Ann. § 646A.602(11)(a)(A)(iv).

<sup>58</sup>Or. Rev. Stat. Ann. § 646A.602(11)(a)(B). As discussed later in this section, Oregon also added, effective January 1, 2016, 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 courts of a financial or other transaction), a consumer’s health insurance policy number or subscriber ID number in combination with any other unique identifier that a health insurer uses to identify a consumer, or any information about a consumer’s medical history or mental or physical condition or about a medical diagnosis or treatment. See *id.* §§ 646A.602(11)(a)(v), 646A.602(11)(a)(vi), 646A.602(11)(a)(vii).

<sup>59</sup>Iowa Code Ann. § 715C.2(1). Iowa defines *breach of security* to mean unauthorized acquisition of personal information maintained in computerized form by a person that compromises the security, confidentiality, or integrity of the personal information. *Id.* § 715C.1(1).

has been acquired has resulted or will result from the breach.”<sup>60</sup>

**New York** simply substitutes an individual’s first name or first initial and last name for “any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person . . . .”<sup>61</sup>

Where data elements are stored separately to minimize the risk of disclosure upon breach, notification may not be required. The **New Jersey** statute, however, provides that “disassociated 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.”<sup>62</sup>

**California’s** security breach statute was amended in 2007 to add medical information and health insurance information,<sup>63</sup> which subsequently have been included in the statutes enacted in **Arizona**,<sup>64</sup> **Colorado**,<sup>65</sup> **Florida**,<sup>66</sup> **Illinois**,<sup>67</sup> **Maryland**,<sup>68</sup> **Missouri**,<sup>69</sup> **North Dakota**,<sup>70</sup> **Rhode**

---

<sup>60</sup>Iowa Code Ann. § 715C.2(6).

<sup>61</sup>N.Y. Gen. Bus. L. § 899-aa(1)(a). These identifiers are defined as *personal information* under the New York statute. **New York** substitutes *private information* for the definition of personal information used in **California** and most other states, defining private information to mean “personal information consisting of any information in combination with 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 . . . .” N.Y. Gen. Bus. L. § 899-aa(1)(b). The elements included in the New York statute are: “(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 . . . .” subject to the standard exclusion for publicly available information. See N.Y. Gen. Bus. L. § 899-aa(1)(b).

<sup>62</sup>N.J. Stat. Ann. § 56:8-161.

<sup>63</sup>Cal. Civ. Code §§ 1798.29(g)(1)(D), 1798.82(h)(1)(D).

<sup>64</sup>See Ariz. Rev. Stat. Ann. § 18-551(11)(f).

<sup>65</sup>See Colo. Rev. Stat. Ann. §§ 6-1-716(g)(I)(A), 24-73-103(1)(e).

<sup>66</sup>Fla. Stat. Ann. §§ 501.171(1)(g)(1)(IV), 501.171(1)(g)(1)(V).

<sup>67</sup>815 Ill. Comp. Stat. Ann. 530/5.

<sup>68</sup>Md. Code Ann., Com. Law §§ 14-3501(e)(1)(i)(4) (health information, including information about an individual’s mental health), 14-3501(e)(1)(i)(5) (a “health insurance policy or certificate number or health

**Island**<sup>71</sup> and **Wyoming**<sup>72</sup> (and **Nevada** includes a variation, a “medical identification number or a health insurance identification number”<sup>73</sup>), although statutes modeled on the original California law generally do not include these data elements. **Arkansas** applies its notification statute to medical information (in both electronic and physical form), **Puerto Rico** includes medical information protected by HIPAA,<sup>74</sup> and **South Dakota** includes health information as defined in 45 C.F.R. § 160.103 (implementing HIPAA).<sup>75</sup>

Under the revised **California** statute, *medical information* is defined to mean “any information regarding an individual’s medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.”<sup>76</sup> *Health insurance information*, in turn, means “an individual’s health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual’s application and claims history, includ-

---

insurance subscriber identification number, in combination with a unique identifier used by an insurer or an employer that is self-insured, that permits access to an individual’s health information . . . .”).

<sup>69</sup>See Mo. Rev. Stat. § 407.1500.1(9).

<sup>70</sup>N.D. Cent. Code §§ 51-30-01(4)(a)(7), 51-30-01(4)(a)(8). *Medical information* means “any information regarding an individual’s medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.” *Id.* § 51-30-01(3).

*Health insurance information* means “an individual’s health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual.” *Id.* § 51-30-01(2).

<sup>71</sup>See R.I. Gen. Laws § 11-49.3-3(a)(8).

<sup>72</sup>See Wyo. Stat. Ann. §§ 6-3-901(b)(xi), 6-3-901(b)(xii), 40-12-501(a)(vii). Wyoming’s statute was amended in 2015 to also add unique biometric data, meaning data generated from measurements or analysis of human body characteristics for authentication purposes, an individual’s taxpayer identification number, a birth or marriage certificate, and a user name or email address, in combination with a password or security question and answer that would permit access to an online account, among other things. See Wyo. Stat. Ann. §§ 6-3-901(b)(ix), 6-3-901(b)(x), 6-3-901(b)(xiii), 40-12-501(a)(vii), 40-12-501(b).

<sup>73</sup>Nev. Rev. Stat. Ann. § 603A.040(1)(d).

<sup>74</sup>10 L.P.R. Ann. § 4051(a)(5).

<sup>75</sup>S.D. Codified Laws § 22-40-19(4)(d).

<sup>76</sup>Cal. Civ. Code §§ 1798.29(h)(2), 1798.82(i)(2).

ing any appeals records.”<sup>77</sup> **Florida** subsequently adopted the same definitions (without using the defined terms) in its statute.<sup>78</sup> **Illinois** employs essentially the same definitions as California, but “medical information” expressly includes information provided to a website or mobile application.<sup>79</sup> **Rhode Island** also adopted the same definitions, except under the Rhode Island statute *Health Insurance Information* is defined as “an individual’s health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual.”<sup>80</sup>

**Delaware** added “[m]edical history, medical treatment by a healthcare professional, diagnosis of mental or physical condition by a health care professional, or deoxyribonucleic acid profile” and a “[h]ealth insurance policy number, subscriber identification number, or any other unique identifier used by a health insurer to identify the person” to its statute effective in 2018.<sup>81</sup>

**Oregon** also amended its notification law effective in 2016 to cover 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 courts of a financial or other transaction), a consumer’s health insurance policy number or subscriber ID number in combination with any other unique identifier that a health insurer uses to identify a consumer, or any information about a consumer’s medical history or mental or physical condition or about a medical diagnosis or treatment.<sup>82</sup>

Pursuant to a 2011 amendment, a covered entity under HIPAA will be deemed to have complied with the require-

---

<sup>77</sup>Cal. Civ. Code §§ 1798.29(h)(3), 1798.82(i)(3).

<sup>78</sup>See Fla. Stat. Ann. §§ 501.171(1)(g)(1)(IV), 501.171(1)(g)(1)(V).

<sup>79</sup>See 815 Ill. Comp. Stat. Ann. 530/5.

<sup>80</sup>R.I. Gen. Laws § 11-49.3-3(a)(3) As amended effective June 26, 2016, *personal information* also is defined to include an “[a]ccount number, credit or debit card number, in combination with any required security code, access code, password or personal identification number that would permit access to an individual’s financial account” and email address “with any required security code, access code, or password that would permit access to an individual’s personal, medical, insurance or financial account.” *Id.* § 11-49.3-3(a)(8).

<sup>81</sup>Del. Code Ann. tit. 6, §§ 12B-101(4)(a)(6), 12B-101(4)(a)(7).

<sup>82</sup>Or. St. §§ 646A.602(11)(a)(v), 646A.602(11)(a)(vi), 646A.602(11)(a)(vii).

ments for the contents of a notice to **California** residents<sup>83</sup> under California's breach notification statute for persons or businesses, if it has complied completely with section 13402(f) of the federal Health Information Technology for Economic and Clinical Health Act, although it will not be exempt from any other provision of the California breach notification statute.<sup>84</sup>

**Virginia** enacted a specific statute requiring notification of a breach of medical information. Under that separate statute, *medical information* is defined to mean

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 Commonwealth, when the data elements are neither encrypted nor redacted:

1. Any information regarding an individual's medical or mental health history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or
2. An individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.<sup>85</sup>

**California** also amended its security breach notification law in 2015, effective January 1, 2016, to include "information or data collected through the use or operation of an automated license plate recognition system."

**Texas** includes information that identifies an individual and relates to: (i) the physical or mental health or condition of the individual; (ii) the provision of health care to the individual; or (iii) payment for the provision of health care to the individual.<sup>86</sup>

Pursuant to amendments that took effect in 2014, **Cali-**

---

<sup>83</sup>See *infra* § 27.08[6].

<sup>84</sup>See Cal. Civ. Code § 1798.82(e). There is no parallel provision for state agencies, which presumably are not also covered entities under HIPAA.

<sup>85</sup>Va. Code Ann. § 32.1-127.1:05(A). *Medical information*, however, 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. *Id.*

<sup>86</sup>Tex. Bus. & Com. Code Ann. § 521.002(a)(2)(B); see also Tex. Gov't Code §§ 205.010, 2054.1125 (applying the same definition to state and local governments).

**California**<sup>87</sup> (and subsequently **Alabama**,<sup>88</sup> **Arizona**, **Colorado**,<sup>89</sup> **Florida**,<sup>90</sup> **Illinois**, **Maryland**,<sup>91</sup> **Nebraska**,<sup>92</sup> and **South Dakota**<sup>93</sup>) created a new category of data elements that would trigger notification obligations (separate and apart from the ones discussed above) where a user name or email address, in combination with a password or security question and answer that would permit access to an online account was or is reasonably believed to have been acquired by an unauthorized person. **Delaware**,<sup>94</sup> **Nevada**<sup>95</sup> and **Wyoming**<sup>96</sup> include security questions and answers, but notification obligations are only triggered if the disclosure is in combination with a user's name or first initial and last name. Most states that impose notification requirements for security questions and answers require that notice of a breach involving login credentials not be sent by email and must instead be sent by another method such as, for example in California and Delaware, "by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an Internet Protocol address or online location from which the person (person or business in California) knows the resident customarily ac-

---

<sup>87</sup>See Cal. Civ. Code §§ 1798.29(g)(2), 1798.82(i)(2).

<sup>88</sup>Ala. Code § 8-38-2(6)(a)(1).

<sup>89</sup>Colo. Rev. Stat. Ann. §§ 6-1-716(1)(g)(I)(B), 24-73-103(g)(I)(B).

<sup>90</sup>Fla. Stat. Ann. §§ 501.171(1)(g)((1)(b), 501.171(4).

<sup>91</sup>Md. Code Ann., Com. Law §§ 14-3501(e)(1), 14-3504(i). Maryland more narrowly added a user name or email address in combination with a password or security question and answer "that permits access to an individual's e-mail account." *Id.* § 14-3501(e)(1)(ii).

<sup>92</sup>Neb. Rev. Stat. § 87-802(5)(b).

<sup>93</sup>S.D. Codified Laws § 22-40-19(5)(a). South Dakota treats as *protected information* both this category (user name or email address, in combination with a password, security question answer, or other information that permits access to an online account) and an "[a]ccount number or credit or debit card number, in combination with any required security code, access code, or password that permits access to a person's financial account . . . ." *Id.* § 22-40-19(5)(b).

<sup>94</sup>Del. Code Ann. tit. 6, § 12B-101(4)(a)(5).

<sup>95</sup>Nev. Rev. Stat. Ann. § 603A.040(1)(e). Nevada more broadly protects a user name, unique identifier or email address in combination with a password, access code or security question and answer that would permit access to an online account.

<sup>96</sup>Wyo. Stat. Ann. §§ 6-3-901(b)(ix), 40-12-501(a)(vii).

cesses the account.”<sup>97</sup> This is a good practice in general, regardless of whether required by state law.

Under the 2014 amendment, California law provides that when no other personal information was involved (*i.e.*, none of the other data elements discussed earlier), notification of a breach may be “in electronic or other form that directs the person whose personal information has been breached to promptly change his or her password and security question or answer (depending on which one was compromised) or take other steps appropriate to protect the online account and all other online accounts for which the person uses the same user name or email address and password or security question or answer.”<sup>98</sup> **Illinois** adopted a variation of this provision, focused on encryption or redaction.<sup>99</sup>

In addition to regular security breach notification obligations, **Washington** further requires notice, and imposes potential liability to financial institutions, where processors, businesses or vendors experience the breach of the security of (i) the full, unencrypted magnetic stripe of a credit card or

---

<sup>97</sup>Cal. Civ. Code §§ 1798.29(i)(5), 1798.82(j)(5); Del. Code Ann. tit. 6, § 12B-102(f); *see also* Md. Code Ann., Com. Law § 14-3504(i) (adopting a similar approach).

<sup>98</sup>Cal. Civ. Code §§ 1798.29(i)(4), 1798.82(j)(4).

<sup>99</sup>*See* 815 Ill. Comp. Stat. Ann. 530/5(2) (“user name or email address, in combination with a password or security question and answer that would permit access to an online account, when either the user name or email address or password or security question and answer are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the data elements have been obtained through the breach of security.”); 815 Ill. Comp. Stat. Ann. 530/10(a)(2) (“With respect to personal information defined in Section 5 in paragraph (2) of the definition of ‘personal information’, notice may be provided in electronic or other form directing the Illinois resident whose personal information has been breached to promptly change his or her user name or password and security question or answer, as applicable, or to take other steps appropriate to protect all online accounts for which the resident uses the same user name or email address and password or security question and answer.”); 815 Ill. Comp. Stat. Ann. 530/12(a)(2) (“With respect to personal information as defined in Section 5 in paragraph (2) of the definition of ‘personal information’, notice may be provided in electronic or other form directing the Illinois resident whose personal information has been breached to promptly change his or her user name or password and security question or answer, as applicable, or to take other steps appropriate to protect all online accounts for which the resident uses the same user name or email address and password or security question and answer. The notification shall not, however, include information concerning the number of Illinois residents affected by the breach.”).

debit card, (ii) the full, unencrypted account information contained in an identification device, or (iii) the unencrypted primary account number on a credit card or debit card or identification device, plus any of the following if not encrypted: cardholder's name, expiration date or service code.<sup>100</sup> This statute is separately analyzed in section 27.08[14].

As noted elsewhere in this section, even where data elements may have been accessed, notification may not be required if the data was encrypted or otherwise obscured or redacted, depending on the applicable state law(s).<sup>101</sup>

### 27.08[3][C] Encryption and Redaction

Most security breach notification statutes focus on whether information or data was potentially accessed in a form in which it could be used to the detriment of affected consumers. Information that is not likely to lead to identity theft or fraud will not trigger a notification obligation in many (but not all) jurisdictions. The particular formulations used, however, differ from state to state and may lead to counter-intuitive results. In some jurisdictions, for example, there may be an obligation to provide notice even if the information was made inaccessible, while in others there may be no obligation to provide notice if it was encrypted, even if the person who acquired the information could have easily decrypted it.

The original **California** statute focused on information that was unencrypted, but now also addresses breaches involving encrypted personal information where the encryption key or security credential was, or is reasonably believed to have been, acquired (if the owner or licensor has a reasonable belief that the encryption key or security credential could render that personal information readable or useable).<sup>1</sup> The current California statute separately imposes additional requirements when email credentials have been compromised.<sup>2</sup> Many state statutes exempt redacted content,

<sup>100</sup>See Wash. Code Ann. § 19.255.020(1)(a).

<sup>101</sup>See *infra* § 27.08[3][C].

#### [Section 27.08[3][C]]

<sup>1</sup>See Cal. Civ. Code §§ 1798.29(a), 1798.82(a).

<sup>2</sup>California law defines *breach of a security system* to mean the “un-

even if it is unencrypted.<sup>3</sup>

Following California's lead, several state statutes focus on the security of keys used to decrypt information. Since 2017, **California** has required notification where encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person if the encryption key or security credential<sup>4</sup> was, or is reasonably believed to have been, acquired by an unauthorized person and the person, business or agency that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that personal information readable or useable.<sup>5</sup> **Colorado** enacted a similar requirement.<sup>6</sup> **Delaware** excludes from

---

authorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by" a person, business or agency, with *personal information* defined to mean "an individual's first name or first initial and last name in combination with any one or more" of specified data elements, "when either the name or the data elements are not encrypted . . . ." Cal. Civ. Code §§ 1798.29(f), 1798.29(g)(1), 1798.82(g), 1798.82(h)(1). The complete versions of these statutory provisions are set forth in section 27.09[6].

As noted in section 27.08[3][B], pursuant to an amendment that took effect in 2014 California also created a separate, independent definition of *personal information* applicable to email account credentials (a user's name or email address, in combination with a password or security question and answer that would permit access to an online account) with special notification requirements to ensure that notice of breach is not provided to an account that has been compromised so that the thief, rather than victim, would receive the notice. *See* Cal. Civ. Code §§ 1798.29(i)(4), 1798.29(i)(5), 1798.29(g)(2), 1798.82(j)(4), 1798.82(j)(5), 1798.82(h)(2).

*Encryption*, since January 1, 2016, has been defined under California law to mean "rendered unusable, unreadable or undecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security."

<sup>3</sup>These jurisdictions include **Arkansas, Guam, Louisiana, Maine, Pennsylvania, South Carolina, Virginia** and **West Virginia**.

<sup>4</sup>*Encryption key* and *security credential* mean "the confidential key or process designed to render the data useable, readable, and decipherable." Cal. Civ. Code §§ 1798.29(l), 1798.82(k).

<sup>5</sup>*See* Cal. Civ. Code §§ 1798.29(a), 1798.82(a).

<sup>6</sup>*See* Colo. Rev. Stat. Ann. §§ 6-1-716(2)(a.4) ("The breach of encrypted or otherwise secured personal information must be disclosed in accordance with this section if the confidential process, encryption key, or other means to decipher the secured information was also acquired in the security breach or was reasonably believed to have been acquired."), 6-1-716(2)(g) ("The breach of encrypted or otherwise secured personal information must be disclosed in accordance with this section if the confidential process,

the definition of *breach of security* the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information if the information is encrypted, “unless such unauthorized acquisition includes, or is reasonably believed to include, the encryption key and the person that owns or licenses the encrypted information has a reasonable belief that the encryption key could render that personal information readable or useable.”<sup>7</sup>

**Alabama** likewise excludes from the definition of *sensitive personally identifying information*, information that has been “truncated, encrypted, secured, or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable, including encryption of the data, document, or device containing the sensitive personally identifying information, unless the covered entity knows or has reason to know that the encryption key or security credential that could render the personally identifying information readable or useable has been breached together with the information.”<sup>8</sup>

**Indiana** requires notification where personal information is encrypted if the information “was or may have been acquired by an unauthorized person with access to the encryption key.”<sup>9</sup> Similarly, **Iowa** defines *personal information* to include information where the name or data elements 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 . . . .”<sup>10</sup> **Texas** defines “breach of a security system” to mean unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information, including “data that is encrypted if the person accessing the data has the key required to decrypt the data.”<sup>11</sup> Under **Minnesota**, **New Hampshire** and **Rhode Island** law, data is not considered

---

encryption key, or other means to decipher the secured information was also acquired or was reasonably believed to have been acquired in the security breach.”).

<sup>7</sup>Del. Code Ann. tit. 6, § 12B-101(1).

<sup>8</sup>Ala. Code § 8-38-2(6)(b)(2).

<sup>9</sup>Ind. Code § 24-4.9-3-1(a)(2).

<sup>10</sup>Iowa Code Ann. § 715C.1(11)(a).

<sup>11</sup>Tex. Bus. & Com. Code Ann. § 521.053(a); *see also* Tex. Gov’t Code §§ 205.010, 2054.1125 (applying the same definition to state and local governments).

encrypted if it is acquired in combination with any required key, security code, or password (or access code, in New Hampshire) that would permit access to the encrypted data.<sup>12</sup> Similarly, **Nebraska** provides that “[d]ata 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 . . . .”<sup>13</sup> **New Mexico**’s statute applies in the event of the unauthorized acquisition of unencrypted computerized data, or of “encrypted computerized data and the confidential process or key used to decrypt the encrypted computerized data, that compromises the security, confidentiality or integrity of personal identifying information maintained by a person.”<sup>14</sup> **South Dakota**’s law uses similar terminology.<sup>15</sup> **Tennessee** generally requires notification where there is a disclosure of unencrypted information or “[e]ncrypted computerized data and the encryption key . . . .”<sup>16</sup> Conversely, information “that has been redacted, or otherwise made unusable . . . .” is excluded from Tennessee’s definition of *personal information*.<sup>17</sup>

**Arizona** and **Colorado** exempt data that is encrypted or redacted (and in the case of Colorado, “secured by any other method rendering the name or the element unreadable”).<sup>18</sup> **Connecticut**, **Mississippi**, **New Jersey** and **North Da-**

<sup>12</sup>See Minn. Stat. Ann. § 325E.61(e) (“‘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 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 . . . .”); 31 N.H. Rev. Stat. Ann. § 359-C:19(II); R.I. Gen. Laws § 11-49.3-3(2).

<sup>13</sup>Neb. Rev. Stat. § 87-802(3).

<sup>14</sup>N.M. Stat. Ann. § 57-12C-2(D).

<sup>15</sup>S.D. Codified Laws § 22-40-19(1) (defining *breach of system security* as “the unauthorized acquisition of unencrypted computerized data or encrypted computerized data and the encryption key by any person that materially compromises the security, confidentiality, or integrity of personal or protected information maintained by the information holder.”).

<sup>16</sup>Tenn. Code Ann. § 47-18-2107(a)(1)(A).

<sup>17</sup>Tenn. Code Ann. § 47-18-2107(a)(4)(B).

<sup>18</sup>See Ariz. Rev. Stat. Ann. §§ 18-552(A), 18-552(L)(1); Colo Rev. Stat. Ann. § 6-1-716(1)(g)(I)(a). Colorado law provides that the breach of “encrypted or otherwise secured personal information” must be disclosed “if the confidential process, encryption key, or other means to decipher the

**kota** exempt personal information “secured by encryption or by any other method or technology that renders the personal information unreadable or unusable . . . ,”<sup>19</sup> while **Minnesota** applies the same formulation but also includes, alternatively, personal information that “was secured and the encryption key, password, or other means necessary for reading or using the data was also acquired.”<sup>20</sup> The **D.C.** statute does not reference encryption, but excludes from disclosure a security breach involving “data that has been rendered secure, so as to be unusable by an unauthorized third party.”<sup>21</sup> **Indiana** includes the Connecticut language as part of its definition of “encryption” for security breaches by individuals or entities (but not government agencies).<sup>22</sup> **Maryland** and **Missouri** use a variation of this language to define personal information, which excludes data elements that are “encrypted, redacted, or otherwise protected by another method that renders the information unreadable or unusable . . . .”<sup>23</sup> **Wisconsin** defines “personal information” to exclude information that is “encrypted, redacted, or altered in any manner that renders the element unreadable . . . .”<sup>24</sup> **Florida** similarly excludes from the definition of personal information “information that is encrypted, secured, or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable.”<sup>25</sup>

**Kentucky** requires disclosure when “unencrypted personal information” (sic)<sup>26</sup> was, or is reasonably believed to have been, acquired by an unauthorized person, but in turn

---

secured information was also acquired or was reasonably believed to have been acquired in the security breach.” Colo. Rev. Stat. Ann. §§ 6-1-716(2)(a.4), 6-1-716(2)(g).

<sup>19</sup>Conn. Gen. Stat. Ann. § 36a-701b(a); Miss. Code Ann. § 75-24-29(2)(a); N.J. Stat. Ann. § 56:8-161; N.D. Cent. Code § 51-30-01(1).

<sup>20</sup>Minn. Stat. Ann. § 325E61(e).

<sup>21</sup>D.C. Code § 28-3851(1).

<sup>22</sup>See Ind. Code § 24-4.9-2-5.

<sup>23</sup>Md. Code Ann., Com. Law § 14-3501(e)(1)(i); Mo. Rev. Stat. § 407.1500.1(9).

<sup>24</sup>Wis. Stat. Ann. § 134.98(1)(b).

<sup>25</sup>Fla. Stat. Ann. § 501.171(1)(g)(2).

<sup>26</sup>It may be assumed that the term *personal information*, as used in section 365.732(2), is a typo and should have been *personally identifiable information*. The Kentucky statute uses the term *personally identifiable information* throughout the statute, and defines it in section 365.732(1)(c),

defines *personally identifiable information* to apply to information when a name or data element is not redacted.<sup>27</sup>

**South Carolina's** security breach statute applies if “unencrypted and unredacted personal information was, or is reasonably likely to have been, acquired by an unauthorized person when the 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 the resident.”<sup>28</sup> Notice is required where the exposure of “computerized data that was not rendered unusable through encryption, redaction, or other methods . . . compromises the security, confidentiality or integrity of personally identifying information . . . , 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 the consumer.”<sup>29</sup>

**Pennsylvania** requires that notice must be provided if encrypted information is accessed and acquired “if the security breach is linked to a breach of the security of the encryption or if the security breach involves a person with access to the encryption key.”<sup>30</sup> **Michigan** requires notification if “unencrypted and unredacted personal information was accessed and acquired by an unauthorized person” or if “personal information was accessed and acquired in encrypted form by a person with unauthorized access to the encryption key.”<sup>31</sup>

**Iowa** requires that notice be given unless the data ele-

---

but imposes the obligation to provide notice when “unencrypted *personal information*” was, or is reasonably believed to have been, acquired by an unauthorized person. Ky. Rev. Stat. Ann. § 365.732(2) (emphasis added). Kentucky's security breach notification law was enacted in 2014, by which time multiple other states had enacted statutes that used the term *personal information*. In all likelihood, the Kentucky legislature, which based section 365.732 on similar statutes previously enacted by other states, left in this term with other language borrowed from another state's law, rather than changing it to *personally identifiable information*.

When Kentucky enacted additional provisions governing security breaches by public agencies and educational institutions, it used the term *personal information*, not *personally identifiable information*. See Ky. Rev. Stat. Ann. §§ 61.931 *et seq.*; *infra* § 27.09[20].

<sup>27</sup>Ky. Rev. Stat. Ann. § 365.732(2).

<sup>28</sup>S.C. Code Ann. §§ 1-11-490(A) (agencies), 39-1-90(A) (persons).

<sup>29</sup>S.C. Code Ann. §§ 1-11-490(D)(2) (agencies), 39-1-90(D)(1) (persons).

<sup>30</sup>73 Pa. Stat. Ann. § 2303(b).

<sup>31</sup>Mich. Comp. Laws Ann. § 445.72(1).

ments were rendered unusable through encryption, redaction or other methods, if the information obtained would be sufficient to permit a person to commit identity theft against the consumer. Iowa's statute excludes data elements that are "encrypted, redacted, or otherwise altered by any method or technology in such a manner that the names or data elements are unreadable,"<sup>32</sup> and is further limited to "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 was subject to a breach . . . ."<sup>33</sup> The same limitation used to apply under **Oregon's** statute, which since 2016 requires notice "if encryption, redaction or other methods have not rendered the data elements unusable or if the data elements are encrypted and the encryption key has also been acquired . . . ."<sup>34</sup>

**Missouri**<sup>35</sup> and **Nebraska**<sup>36</sup> exempt material that is "encrypted, redacted, or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable . . . ." They define *encryption* to mean (in the case of Nebraska, "converted by," for Missouri, simply "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.<sup>37</sup> *Encryption* is defined the same way under **Vermont** law.<sup>38</sup>

*Redact* under **Nebraska** law means "to alter or truncate data such that no more than the last four digits of a Social Security number, motor vehicle operator's license number,

---

<sup>32</sup>Iowa Code Ann. § 715C.1(11)(a).

<sup>33</sup>Iowa Code Ann. § 715C.2(1) (emphasis added). Iowa defines breach of security to mean unauthorized acquisition of personal information maintained in computerized form by a person that compromises the security, confidentiality, or integrity of the personal information. Iowa Code Ann. § 715C.1(1). In addition, as discussed above in section 27.08[3][A], notification is not required if there is no reasonable likelihood of financial harm, which further narrows its scope.

<sup>34</sup>Or. St. § 646A.602(11)(a)(A).

<sup>35</sup>Mo. Rev. Stat. §§ 407.1500.1(4), 407.1500.1(9).

<sup>36</sup>Neb. Rev. Stat. § 87-802(5)(a).

<sup>37</sup>As noted earlier, however, Nebraska amended its security breach law effective July 2016 to provide that 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).

<sup>38</sup>See Vt. Stat. Ann. tit. 9, § 2430(7).

state identification card number, or account number is accessible as part of the personal information.”<sup>39</sup> **Ohio** defines *redacted* in substantially the same way.<sup>40</sup> **Guam, Oklahoma** (for breaches involving individuals and entities, but not state agencies) and **Virginia** also define *Redact* substantially the same way except that in addition to the last four digits of a driver’s license, state identification card number or account number, any five digits of a Social Security number may be visible.<sup>41</sup>

*Redact* is defined under **Indiana**<sup>42</sup> and **Kansas**<sup>43</sup> law specifically to mean “alteration or truncation of data such that no more than” five digits of a Social Security number or the last four digits of a driver’s license, state identification card or account number “are accessible as part of the personal information . . . .” **Michigan** employs a substantially similar definition (“to alter or truncate data . . . .”) but the minimum digits exposed that would still allow a company to treat the data as redacted is stated differently (“no more than four sequential digits of a driver’s license number, state personal identification card number, or account number, or no more than five sequential digits of a Social Security number”).<sup>44</sup> *Redact* under **Pennsylvania** and **West Virginia** law are substantially similar to the definition provided under Kansas and Michigan law, except that only the last four—not five—digits may be displayed.<sup>45</sup>

**Wyoming**’s statute does not even reference encryption. Instead, it simply provides that *personally identifying information* means the first name or first initial and last name in combination with one or more data elements (Social Security number; driver’s license or Wyoming identification card; 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; tribal identification card; or federal or state government issued identification card) that are not redacted. *Redact* is

---

<sup>39</sup>Neb. Rev. Stat. § 87-802(6).

<sup>40</sup>See Ohio Rev. Code § 1347.12(A)(8).

<sup>41</sup>Okla. Stat. Ann. tit. 24, § 162(8); Va. Code Ann. § 18.2-186.6(A).

<sup>42</sup>Ind. Ann. Code § 24-4.9-2-11.

<sup>43</sup>Kan. Stat. Ann. § 50-7a01(d).

<sup>44</sup>Mich. Comp. Laws Ann. § 445.63(r).

<sup>45</sup>73 Pa. Stat. Ann. § 2302; W. Va. Code § 46A-2A-101(8).

define to mean “alteration or truncation of data such that no more than five (5) digits of the data elements provided [other than the federal or state government issued identification card] . . . are accessible as part of the personal information . . . .”<sup>46</sup> It is noteworthy that the definition of *redact* in Wyoming is not focused on merely the last five digits of a data element or even five consecutive digits.

**Hawaii** and **North Carolina** exclude encrypted or redacted data, with redacted defined to mean “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.”<sup>47</sup> **Vermont** uses a similar definition for redaction (“the rendering of data so that the data are unreadable or are truncated so that no more than the last four digits of the identification number are accessible as part of the data”) and excludes from the definition of *personally identifiable information* material that is “encrypted, redacted, or protected by another method that renders the information unreadable or unusable by an unauthorized persons . . . .”<sup>48</sup>

As noted earlier in this section, **Alabama**—which only enacted a security breach law in 2018 and therefore benefited by reviewing earlier enacted statutes—excludes information that is “truncated, encrypted, secured, or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders

<sup>46</sup>Wyo. Stat. Ann. §§ 40-12-501(a)(vii), 40-12-501(a)(viii). The definition of *redact* in section 40-12-501(a)(viii) still refers to the data elements that prior to July 1, 2015, were enumerated in section 40-12-501(a)(vii)(A) through (D), which were all of the data elements codified at that time other than a federal or state issued identification card (which was identified in section 40-12-501(a)(vii)(E)). Prior to July 1, 2015, this meant that notice was not required if the data elements listed in subparts (A) through (D) were redacted, but *was* still required even if five or fewer digits of a federal or state issued identification card were exposed. In 2015, Wyoming expanded the list of data elements, which are now codified at Wyo. Stat. Ann. §§ 6-3-901(b)(iii) through (xiv). Because section 501(a)(viii) still refers to the pre-July 1, 2015 numbering scheme, rather than to some or all of the data elements now codified in section 6-3-901(b)(iii) through (xiv), it is unclear whether notice still is required when even redacted federal or state identification card numbers are disclosed.

<sup>47</sup>Haw. Rev. Stat. Ann. § 487N-1; N.C. Gen. Stat. § 75-61(13).

<sup>48</sup>Vt. Stat. Ann. tit. 9, § 2430(9)(A), 2430(11). Prior to 2012, Vermont’s security breach statute applied to *personal information* rather than *personally identifiable information*, although the newer term is defined coextensively with the old definition of *personal information*.

the information unusable, including encryption of the data, document, or device containing the sensitive personally identifying information, unless the covered entity knows or has reason to know that the encryption key or security credential that could render the personally identifying information readable or useable has been breached together with the information.”<sup>49</sup> It also defines *sensitive personally identifying information* to include, among other things, a non-truncated Social Security number or tax identification number, or a non-truncated driver’s license number, state-issued identification card number, passport number, military identification number, or other unique identification number issued on a government document used to verify the identity of a specific individual.<sup>50</sup>

Statutes enacted more recently generally define *encryption* based on best practices or objective third party criteria, while older statutes are less exacting or focus on a low probability of decryption. Two states—Massachusetts and Rhode Island—define encryption in terms of specific technology, as discussed later in this section. As statutes are amended, state legislatures borrow from one another. They also make minor edits, as reflected, for example, in the fact that a number of states define encryption in terms of information that is *indecipherable*, while others use the term *undecipherable*.

The **Utah** security breach statute does not define encryption but it provides that *personal information* includes information where “either the name or data element is unencrypted or not protected by another method that renders the data unreadable or unusable . . . .”<sup>51</sup>

*Encryption* or *encrypted* is defined under the laws of **Guam, Kansas, Michigan, Oklahoma** (for incidents involving individuals and entities, not government agencies), **New Hampshire, Virginia**, and **West Virginia** to mean substantially “the transformation of data through the use of an algorithmic process into a form for which<sup>52</sup> there is a low probability of assigning meaning without use of a confidential process or key, or securing the information by another

---

<sup>49</sup>Ala. Code §§ 8-38-2(6)(b)(2).

<sup>50</sup>Ala. Code §§ 8-38-2(6)(a)(1), 8-38-2(6)(a)(2).

<sup>51</sup>See Utah Code Ann. § 13-44-102(3)(a).

<sup>52</sup>Some statutes use “in which” rather than “for which.”

method that renders the data elements unreadable or unusable.”<sup>53</sup> **Indiana, Ohio** and **Pennsylvania** similarly define *encryption* as “the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key.”<sup>54</sup>

**Indiana’s** statute was amended in 2008 to tighten this definition. The law now provides that to be deemed *encrypted* under the statute, data must have been transformed 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 secured by another method that renders the data unreadable or unusable, provided that these processes are undertaken “in a manner consistent with the best practices common in the industry . . . .”<sup>55</sup> The statute further provides that data encrypted in this manner is not deemed *encrypted* for purposes of the statute “unless the key required to decrypt the data complies with the best practices common in the industry and has not been disclosed or compromised.”<sup>56</sup>

**California**, since 2016, has defined *encrypted* to mean “rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security.”<sup>57</sup> Thereafter, **Colorado**<sup>58</sup> and **New Mexico**<sup>59</sup> adopted this definition and **Delaware** enacted essentially

<sup>53</sup>9 Guam Code Ann. § 48.20(c); Kan. Stat. Ann. § 50-7a01(b); Mich. Comp. Laws Ann. § 445.63(g); Okla. Stat. Ann. tit. 24, § 162(3); 31 N.H. Rev. Stat. Ann. § 359-C:19(II) (“completely unreadable or unusable”); Va. Code Ann. § 18.2-186.6(A); W. Va. Code Ann. § 46A-2A-101(3); *see also* Va. Code Ann. § 32.1-127.1:05(a) (governing security breaches involving medical information).

<sup>54</sup>Ind. Code § 24-4.9-2-5(1); Ohio Rev. Code § 1347.12(A)(4); 73 Pa. Stat. Ann. § 2302. As noted earlier in the text, Indiana alternatively provides that data is encrypted for purposes of its notification statute if the data “are secured by another method that renders the data unreadable or unusable.” Ind. Code § 24-4.9-2-5(2).

<sup>55</sup>Ind. Code § 24-4.9-2-5(a).

<sup>56</sup>Ind. Code § 24-4.9-2-5.

<sup>57</sup>Cal. Civ. Code §§ 1798.29(h)(4), 1798.82(i)(4).

<sup>58</sup>Colo. Rev. Stat. Ann. § 6-1-716(1)(d).

<sup>59</sup>*See* N.M. Stat. Ann. § 57-12C-2(B).

the same definition (minus “to an unauthorized person”).<sup>60</sup>

**Maryland** revised its statute in 2017 to define *encrypted* to mean “protection of data in electronic or optical form using an encryption technology that renders the data indecipherable without an associated cryptographic key necessary to enable decryption of the data.”<sup>61</sup>

Most statutes do not mandate a particular level of encryption. **Massachusetts**, however, defines *encrypted* to mean 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 . . . .”<sup>62</sup> However, the Massachusetts department of consumer affairs and business regulation has authority to revise that definition over time.<sup>63</sup> Given how rapidly technologies advance, what constitutes strong encryption today is likely to be viewed as weak at a later point in time.<sup>64</sup> Indeed, today 128-bit encryption is not considered strong encryption.

**Rhode Island**, like Massachusetts, requires 128-bit or higher encryption by defining encrypted to mean “the transformation of data through the use of a one hundred twenty-eight (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.”<sup>65</sup> Since a notification obligation is triggered by unauthorized access to

<sup>60</sup>Del. Code Ann. tit. 6, § 12B-101.

<sup>61</sup>Md. Code Ann., Com. Law § 14-3501(c). The companion law governing security breaches by state agencies defines *encrypted* as the protection of data in electronic or optical form, in storage or in transit, using a technology that:

(1) is certified to meet or exceed the level that has been adopted by the Federal Information Processing Standards issued by the National Institute of Standards and Technology; and

(2) renders such data indecipherable without an associated cryptographic key necessary to enable decryption of such data.

Md. Code Ann., State Gov’t § 10-1301(b). This is similar to the standard applied under Nevada law in connection with breaches involving credit card data. See Nev. Rev. Stat. Ann. § 603A.215(5)(b).

<sup>62</sup>Mass. Gen. L. Ann. ch. 93H, § 1.

<sup>63</sup>See Mass. Gen. L. Ann. ch. 93H, §§ 1, 3.

<sup>64</sup>See generally *supra* § 27.03.

<sup>65</sup>R.I. Gen. Laws § 11-49.3-3(a)(2). Data will 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.” *Id.*

or acquisition of *unencrypted* data, Rhode Island's definition of *encrypted* means that even some encrypted data will be treated as unencrypted for purposes of its security breach notification law.

By contrast, **Iowa**'s statute defines *encryption* as "the use of an algorithmic process *pursuant to accepted industry standards* to transform data into a form in which the data is rendered unreadable or unusable without the use of a confidential process or key."<sup>66</sup>

**South Dakota** applies a hybrid definition, treating as *encrypted*, "computerized data that is rendered unusable, unreadable, or indecipherable without the use of a decryption process or key or in accordance with the Federal Information Processing Standard 140-2 in effect on January 1, 2018 . . . ."<sup>67</sup>

**Washington** defines *secured* in its security breach notification law to mean "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."<sup>68</sup> **Kentucky** adopted a variation on Washington's approach for breaches involving government agencies, defining *encryption* to mean "the conversion of data using technology that: (a) Meets or exceeds the level adopted by the National Institute of Standards Technology as part of the Federal Information Processing Standards: and (b) Renders the data indecipherable without the associated cryptographic key to decipher the data . . . ."<sup>69</sup> **Tennessee** similarly amended its definition of *encrypted* to mean "computerized data that is rendered unusable, unreadable, or indecipherable without the use of a decryption process or key and in accordance with the current version of the Federal Information Processing Standard (FIPS) 140-2 . . . ."<sup>70</sup>

### 27.08[3][D] Data on Password-Protected Laptops

**Indiana** previously excluded from the definition of *breach*

---

<sup>66</sup>Iowa Code Ann. § 715C.1(5) (emphasis added).

<sup>67</sup>S.D. Codified Laws § 22-40-19(2).

<sup>68</sup>See Wash. Rev. Code Ann. § 19.255.010(7); Wash. Rev. Code Ann. § 42.56.590(7).

<sup>69</sup>Ky. Rev. Stat. Ann. § 61.931(3).

<sup>70</sup>Tenn. Code Ann. § 47-18-2107(a)(2).

*of the security of a system* “[u]nauthorized 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.”<sup>1</sup> However, effective in 2008, this provision was modified to exclude “[u]nauthorized acquisition of a portable electronic device on which personal information is stored, *if all personal information on the device is protected by encryption* and the encryption key: (A) has not been compromised or disclosed; and (B) is not in the possession of or known to the person who, without authorization, acquired or has access to the portable electronic device.”<sup>2</sup> Hence, password protection alone will no longer be sufficient under Indiana law when a laptop or other mobile device is lost or stolen.

While other statutes do not contain an express exclusion for information or data that is password-protected, as noted above in section 27.08[3][C] some security breach statutes provide that notice to consumers need not be given unless a security incident is reasonably likely to lead to unauthorized access. Whether a security incident is *likely* to lead to unauthorized access in a given case may be subject to differing interpretations. Depending on the nature of the breach and the sophistication of the thief, if discernible, these statutes potentially could allow a business to avoid providing notification where otherwise unencrypted, unredacted data was password protected.<sup>3</sup>

### 27.08[3][E] Electronic vs. Paper Records and Audio Recordings

Most security breach notification statutes apply only to electronic data and information. However, for security breaches by individuals or entities (but not state agencies), **Indiana** extends coverage to “computerized data that have been transferred to another medium, including paper, microfilm, or a similar medium, even if the transferred data

---

#### [Section 27.08[3][D]]

<sup>1</sup>Ind. Code § 24-4.9-2-2(b)(2) (2006).

<sup>2</sup>Ind. Code § 24-4.9-2-2(b)(2) (emphasis added).

<sup>3</sup>A sophisticated hacker could likely circumvent password protection. A laptop taken during a break in focused on items that would be easy to quickly resell might have been stolen by someone interested in or able to circumvent password protection. Of course, the specific facts of each data breach would need to be closely evaluated.

are no longer in a computerized format.”<sup>1</sup> **Iowa** defines breach of security to mean “unauthorized acquisition of personal information maintained by a person in any medium, including on paper, that was transferred by the person to that medium from computerized form and that compromises the security, confidentiality, or integrity of the personal information.”<sup>2</sup>

**Hawaii**<sup>3</sup> and **North Carolina**<sup>4</sup> more broadly require notice of security breaches when personal information in any form (“whether computerized, paper, or otherwise”) has been compromised. Similarly, effective in 2015, **Washington** deleted reference to *computerized* in its security breach notification statutes, making the laws applicable to data generally (including paper records).<sup>5</sup> **Alaska** effectively has the same coverage because it applies to acquisition by (A) photocopying, facsimile, or other paper-based method; (B) a device, including a computer, that can read, write, or store information that is represented in numerical form; or (C) a method not identified by (A) or (B) of this paragraph.<sup>6</sup>

**Arkansas** applies its notification statute to medical information in physical, as well as electronic form.

**D.C.**’s security breach statute applies to “computerized or other electronic data, or any equipment or device storing such data . . . .”<sup>7</sup> **Massachusetts** similarly defines data broadly to mean “any material upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved regardless of physical form or characteristics.”<sup>8</sup>

**Georgia** enacted a statute separate from its regular secu-

---

[Section 27.08[3][E]]

<sup>1</sup>Ind. Code § 24-4.9-2-2(a).

<sup>2</sup>Iowa Code Ann. § 715C.1(1).

<sup>3</sup>Haw. Rev. Stat. Ann. § 487N-2(a).

<sup>4</sup>N.C. Gen. Stat. § 75-65(a).

<sup>5</sup>See Wash. Rev. Code Ann. § 19.255.010(1); Wash. Rev. Code Ann. § 42.56.590 (1)(a).

<sup>6</sup>Alaska Stat. § 45.48.090(1).

<sup>7</sup>D.C. Code § 28-3851(1).

<sup>8</sup>Mass. Gen. L. Ann. ch. 93H, § 1. Massachusetts defines breach of security to include the unauthorized acquisition or use of unencrypted data or encrypted electronic data and confidential process or key that is capable of compromising the security, confidentiality, or integrity of

rity breach notification law, requiring notification from telecommunication companies of any breach of a telephone record concerning a Georgia resident.<sup>9</sup> The statute is reprinted in section 27.09[12].

**27.08[3][F] Exclusion: Publicly Available Information and Truncated Identification Numbers**

Publicly available information that is lawfully made available to the general public from federal, state or local government records generally is exempted from the definition of *personal information* (or whatever comparable term is used)<sup>1</sup> (or under the **Massachusetts** and **South Carolina** statutes, “information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public,”<sup>2</sup> in **Michigan**, “federal, state, or local government records or documents lawfully made available to the general public,”<sup>3</sup> in the case of **Oregon**’s statute, “information in a federal, state or local government record, other than a Social Secu-

---

personal information. *See* Mass. Gen. L. Ann. ch. 93H, § 1. *Electronic* is defined as “relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities.” Mass. Gen. L. Ann. ch. 93H, § 1. The statute’s definition of data and reference to data as opposed to electronic data underscores that it was intended to extend beyond merely electronic data breaches.

<sup>9</sup>*See* Ga. Code Ann. § 46-5-214; *infra* § 27.09[12].

**[Section 27.08[3][F]]**

<sup>1</sup>*See, e.g.*, Cal. Civ. Code. §§ 1798.29(h)(1), 1798.82(i)(1); *see also, e.g.*, Ala. Code § 8-38-2(6)(b)(1) (excluding “[i]nformation about an individual which has been lawfully made public by a federal, state, or local government record or a widely distributed media.”); D.C. Code § 28-3851(3)(B); Fla. Stat. Ann. § 501.171(1)(g)(2) (excluding “information about an individual that has been made publicly available by a federal, state, or local governmental entity.”); Ind. Code. § 24-4.9-2-10(2); Md. Code Ann., Com. Law § 14-3501(e)(2)(i); Miss. Code Ann. § 75-24-29(2)(b)(iii); Mo. Rev. Stat. § 407.1500.1(9)(f); Neb. Rev. Stat. § 87-802(5)(iii); 31 N.H. Rev. Stat. Ann. § 359-C:19(V); S.D. Codified Laws § 22-40-19(4); Tex. Bus. & Com. Code Ann. § 521.002(b) (exclusion from the definition of sensitive personal information); Tex. Gov’t Code §§ 205.010, 2054.1125 (state and local governments); Vt. Stat. Ann. tit. 9, § 2430(5)(C)(iv); Vt. Stat. Ann. tit. 9, § 2430(9)(B); Va. Code Ann. § 18.2-186.6(A); V.I. Code Ann. tit. 14, §§ 2208(f) (agencies), 2209(f) (persons and businesses).

<sup>2</sup>Mass. Gen. L. Ann. ch. 93H, § 1; S.C. Code Ann. § 39-1-90(D)(3)(d).

<sup>3</sup>Mich. Comp. Laws Ann. § 445.72(17).

rity number, that is lawfully available to the public”<sup>4</sup>) or in the case of **Alabama**, “[t]he release of a public record not otherwise subject to confidentiality or nondisclosure requirements.”<sup>5</sup>

Many statutes also exclude the last four<sup>6</sup> or five<sup>7</sup> digits of a person’s Social Security number (or in the case of **Guam, Indiana** and **Virginia** any five digits of a Social Security number)<sup>8</sup> or the last four digits of a person’s driver’s license or state identification number<sup>9</sup> or account number<sup>10</sup> or in the case of **Wyoming** any five digits (not merely the last) of any of these data elements or a tribal identification card (and potentially others).<sup>11</sup>

<sup>4</sup>Or. St. § 646A.602(11)(b).

<sup>5</sup>Ala. Code § 8-38-2(B)(1). Nondisclosure agreements separately are analyzed in chapter 10 in connection with trade secret law. *See generally supra* § 10.04[3].

<sup>6</sup>*See, e.g.*, 3 Ind. Code § 4-1-11-3 (applicable to government agencies); Or. St. § 646A.602(15).

<sup>7</sup>*See* Mo. Rev. Stat. § 407.1500.1(10).

<sup>8</sup>*See* 9 Guam Code Ann. § 48.20(h)(1); Ind. Code Ann. § 24-4.9-2-11(b); Va. Code Ann. § 18.2-186.6(A) (defining *redact*).

<sup>9</sup>Nev. Rev. Stat. Ann. § 603A.040.

<sup>10</sup>*See* Ind. Code. § 24-4.9-2-11; Mo. Rev. Stat. § 407.1500.1(10); Ore. St. § 646A.602(15); *see also* Va. Code Ann. § 18.2-186.6(A) (defining *redact* to mean, among other things, alteration or truncation of data such that no more than the last four digits of a driver’s license number, state identification card number or account number are accessible); *see also* Mo. Rev. Stat. § 407.1500.1(10) (using a similar definition of *redact* except limited to the last five Social Security numbers or the last four numbers from a driver’s license, state identification card or account number).

<sup>11</sup>*See* Wyo. Stat. Ann. § 40-12-501(a)(viii). The definition of *redact* in section 40-12-501(a)(viii) still refers to the data elements that prior to July 1, 2015, were enumerated in section 40-12-501(a)(vii)(A) through (D), which were all of the data elements codified at that time other than a federal or state issued identification card (which was identified in section 40-12-501(a)(vii)(E)). Prior to July 1, 2015, this meant that notice was not required if the data elements listed in subparts (A) through (D) were redacted, but *was* still required even if five or fewer digits of a federal or state issued identification card were exposed. In 2015, Wyoming expanded the list of data elements, which are now codified at Wyo. Stat. Ann. §§ 6-3-901(b)(iii) through (xiv). Because section 501(a)(viii) still refers to the pre-July 1, 2015 numbering scheme, rather than to some or all of the data elements now codified in section 6-3-901(b)(iii) through (xiv), it is unclear whether notice still is required when even redacted federal or state identification card numbers are disclosed. Further, as a result of this error, it is also unclear whether the definition of *redact* applies to any of the

**Maryland** further excludes “[i]nformation that an individual has consented to have publicly disseminated or listed” and information that is disseminated or listed in accordance with the federal Health Insurance Portability and Accountability Act.<sup>12</sup> **North Carolina** excludes “electronic identification numbers, electronic mail names or addresses, Internet account numbers, Internet identification names, parent’s legal surname prior to marriage, or a password unless this information would permit access to a person’s financial account or resources.”<sup>13</sup> Likewise, it excludes “publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, including name, address, and telephone number . . . .”<sup>14</sup>

**Ohio** further expressly excludes information compiled in news reports, in connection with news gathering, or in charitable publications.<sup>15</sup>

**Utah** and **Wyoming** exclude 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.”<sup>16</sup> **Mississippi** likewise excludes “publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media . . . .”<sup>17</sup>

**Puerto Rico**’s statute is narrower than most, excluding only mailing or residential addresses from the definition of *personal information file* if these addresses are included in a generally available public document.<sup>18</sup>

### 27.08[3][G] Exclusion: Criminal Intelligence Systems

Even if a breach otherwise would trigger notification obligations, under **Virginia** law a breach involving criminal

---

new data elements added by Wyoming in 2015.

<sup>12</sup>See Md. Code Ann., Com. Law § 14-3501(e)(2)(ii), 14-3501(e)(2)(iii).

<sup>13</sup>N.C. Gen. Stat. § 75-65(a).

<sup>14</sup>N.C. Gen. Stat. § 75-61(10).

<sup>15</sup>See Ohio Rev. Code § 1347.12(A)(6) (enumerating a number of express exemptions).

<sup>16</sup>Utah Code Ann. § 13-42-102(3)(b); Wyo. Stat. Ann. § 40-12-501(b).

<sup>17</sup>Miss. Code Ann. § 75-24-29(2)(b)(iii).

<sup>18</sup>10 L.P.R. Ann. § 4051(a).

intelligence systems subject to the restrictions of 28 C.F.R. Part 23 that are maintained by law enforcement agencies in Virginia and the organized Criminal Gang File of the Virginia Criminal Information Network (VCIN), established pursuant to Va. Code Ann. § 52-12, are exempted from the obligations of the Virginia security breach notification statute.<sup>1</sup>

#### **27.08[4] The Timing of Notification and Pre-Notice Obligations**

If there is an obligation to provide notice to consumers, most statutes establish normative, rather than set deadlines for providing notice. As discussed later in this subsection, however, some state laws require notice to be sent by specific deadlines that may be as short as 30 days from the time a determination is made that a breach has occurred (or the time a person or entity has reason to believe that a breach occurred). Some states also impose pre-notice obligations that may affect the timing of notice, including potential duties to investigate the breach, file a police report and/or obtain police consent to provide notification. Some statutes mandate delay to accommodate the needs of law enforcement, while others merely permit it or do not even necessarily account for it. Where a breach occurs as a result of acquisition of information over a period of time by the same person or entity, the series of events may be treated as a single breach under **Alabama** law<sup>1</sup> (and generally, as a practical matter, in all states, assuming that the intrusions are related).<sup>2</sup>

Under the **California** statute, a person or business that maintains computerized data that includes personal information that the person or business does not own must notify the owner or licensee “immediately following discovery, if the personal information was, or is reasonably believed to

---

#### **[Section 27.08[3][G]]**

<sup>1</sup>See Va. Code Ann. § 18.2-186.6(L).

#### **[Section 27.08[4]]**

<sup>1</sup>See Ala. Code § 8-38-2(1).

<sup>2</sup>Insurance law may define, for purposes of coverage, whether multiple intrusions are independent or part of a continuing or ongoing event.

have been, acquired by an unauthorized person.”<sup>3</sup> Owners and licensees, in turn, must provide notice “following<sup>4</sup> discovery or notification . . . in the most expedient time possible and without unreasonable delay,<sup>5</sup> consistent with the legitimate needs of law enforcement . . . .”<sup>6</sup> **Iowa** similarly requires that notice be provided “in the most expeditious manner possible and without unreasonable delay . . . .” (consistent with the legitimate needs of law enforcement and any measures necessary to sufficiently determine contact information for the affected consumers, determine the scope of the breach, and restore the reasonable integrity, security

---

<sup>3</sup>Cal. Civ. Code §§ 1798.29(b), 1798.82(b). While this is also the standard for notice by data owners or licensees under Georgia law, 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 notify the information broker or data collector of any breach within twenty-four hours following discovery if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Ga. Code Ann. § 10-1-912(b).

Under **Oklahoma** (for individuals and entities, but not state agencies) and **West Virginia** law, notice to an owner or licensee need only be provided “as soon as practicable following discovery, if the personal information was or if the entity reasonably believes [sic] was accessed and acquired by an unauthorized person.” Okla. Stat. Ann. tit. 24, § 163(C); W. Va. Code § 46A-2A-102(c) (emphasis added).

Similar to West Virginia’s statute, **Wyoming** provides that any person who maintains computerized data that includes personally identifying information of another business entity must disclose to the business entity for which the information is maintained any breach of the security of the system “as soon as practicable following the determination that personal information was, or is reasonably believed to have been, acquired by an unauthorized person.” Wyo. Stat. Ann. § 40-12-502(g). The statute further provides that the person who maintains the data on behalf of another business entity and the business entity on whose behalf the data is maintained may agree which person or entity will provide any required notice to consumers (and only one notice to consumers is required). *Id.* If agreement cannot be reached, “the person who has the direct business relationship with the resident . . . shall provide notice . . . .” *Id.*

<sup>4</sup>**New Jersey** modifies “following” to read “immediately following.” See N.J. Stat. Ann. § 56:8-163(b). **The District of Columbia** modifies California’s language by changing “following” to “promptly” (and modifying the sentence in light of that change). See D.C. Code § 28-3852(a).

<sup>5</sup>This language is also used in **New York**’s security breach notification statute, N.Y. Gen. Bus. L. § 899-aa(1)(c).

<sup>6</sup>Cal. Civ. Code §§ 1798.29(a), 1798.82(a). **Kentucky** employs the same language. See Ky. Rev. Stat. Ann. § 365.732(2).

and confidentiality of the data).<sup>7</sup>

**Florida**, subject to an outer limit of 30 days generally requires that notice be made “as expeditiously as practicable and without unreasonable delay, taking into account the time necessary to allow the covered entity to determine the scope of the breach of security, to identify individuals affected by the breach, and to restore the reasonable integrity of the data system that was breached . . . .”<sup>8</sup> **Alabama** adopted Florida’s statute, but extended the outside time limit to 45 days, and also sets in greater detail than the laws of other states the specific steps that a covered entity should undertake to determine if there was a breach,<sup>9</sup> which is discussed in more detail later in this subsection. A third party agent<sup>10</sup> under Alabama law, must notify the covered entity<sup>11</sup> of the breach “as expeditiously as possible and without unreasonable delay” but in no case later than 10 days following the determination or reason to believe that a

---

<sup>7</sup>Iowa Code Ann. § 715C.2(1). **Ohio** requires notice in an expeditious manner. *See* Ohio Rev. Code § 1347.12(C) (state agencies); Ohio Rev. Code § 13499.19(C). Expeditious notice is an objective noted in the legislative findings of the **Georgia** and **Louisiana** security breach notification statutes, although the laws themselves merely mandate disclosure following discovery or notice of breach. *See* Ga. Code Ann. § 10-1-910(7); La. Stat. Ann. § 51:3072(5).

<sup>8</sup>Fla. Stat. Ann. § 501.171(4)(a). Notice must be delayed, however, if a federal, state or local law enforcement agency determines that notice to individuals would interfere with a criminal investigation, upon the written request of the law enforcement agency for a specified period that the law enforcement agency determines is reasonably necessary. *Id.* § 501.171(4)(b).

<sup>9</sup>*See* Ala. Code §§ 8-38-4, 8-38-5(b). Subject to the investigation required by section 8-38-4 and the potential for delay set forth in section 8-38-5(c) (discussed later in this section), section 8-38-5(b) requires notice within 45 days “of the covered entity’s receipt of notice from a third party agent that a breach has occurred or upon the covered entity’s determination that a breach has occurred and is reasonably likely to cause substantial harm to the individuals to whom the information relates.” *Id.* § 8-38-5(b).

<sup>10</sup>A *third party agent* is defined as an “entity that has been contracted to maintain, store, process, or is otherwise permitted to access sensitive personally identifying information in connection with providing services to a covered entity.” Ala. Code § 8-38-2(7).

<sup>11</sup>A *covered entity* is defined as a “person, sole proprietorship, partnership, government entity, corporation, nonprofit, trust, estate, cooperative association, or other business entity that acquires or uses sensitive personally identifying information.” Ala. Code § 8-38-2(2).

breach occurred.<sup>12</sup>

**Guam**,<sup>13</sup> **Michigan** and **Indiana**<sup>14</sup> require that notice merely be made “without unreasonable delay.”<sup>15</sup> **Massachusetts** requires notice “as soon as practicable and without unreasonable delay” when a person or agency knows or has reason to know (1) of a security breach or (2) that personal information was acquired or used by an unauthorized person or used for an unauthorized purpose.<sup>16</sup> **Texas** simply requires that notice be provided “as quickly as possible” (except as necessary to determine the scope of the breach and restore the reasonable integrity of the data system or as requested by law enforcement so as not to impede a criminal investigation).<sup>17</sup>

All state statutes assume some level of investigation will be required to determine whether a breach occurred and notice to consumers will be required. Some states, however, expressly mandate an initial investigation following notice or discovery of a breach to determine whether notice must be sent or falls within an exemption and, as noted earlier, as of late 2018 Alabama laid out the most detailed requirements of any state security breach notification law. Under **Alabama** law, a covered entity must “conduct a good faith and prompt investigation” that includes all of the following:

- (1) An assessment of the nature and scope of the breach.

---

<sup>12</sup>Ala. Code § 8-38-8.

<sup>13</sup>9 Guam Code Ann. § 48.30(a).

<sup>14</sup>Ind. Code § 24-4.9-3-3(a) (consumer notice). Under the statute, a delay is reasonable if the delay is:

- (1) necessary to restore the integrity of the computer system;
- (2) necessary to discover the scope of the breach; or
- (3) in response to a request from the attorney general or a law enforcement agency to delay disclosure because disclosure will:
  - (A) impede a criminal or civil investigation; or
  - (B) jeopardize national security.

*Id.*

<sup>15</sup>Mich. Comp. Laws Ann. § 445.72(4).

<sup>16</sup>Mass. Gen. L. Ann. ch. 93H, § 3. Subsection (A) provides for notice by a person or agency that stores but does not own or license data to the owner or licensor. Subsection (B) provides for notice by a person or agency that owns or licenses data to affected state residents, the Attorney General and the director of consumer affairs and business regulation.

<sup>17</sup>Tex. Bus. & Comm. Code § 521.053(b); *see also* Tex. Gov’t Code §§ 205.010, 2054.1125 (applying section 521.053(b) to state and local governments).

- (2) Identification of any sensitive personally identifying information that may have been involved in the breach and the identity of any individuals to whom that information relates.
- (3) A determination of whether the sensitive personally identifying information has been acquired or is reasonably believed to have been acquired by an unauthorized person, and is reasonably likely to cause substantial harm to the individuals to whom the information relates.
- (4) Identification and implementation of measures to restore the security and confidentiality of the systems compromised in the breach.<sup>18</sup>

The statute also lays out specific circumstances that may be considered “[i]n determining whether sensitive personally identifying information has been acquired or is reasonably believed to have been acquired by an unauthorized person without valid authorization . . . .”<sup>19</sup> Those factors are:

- (1) Indications that the information is in the physical possession and control of a person without valid authorization, such as a lost or stolen computer or other device containing information.
- (2) Indications that the information has been downloaded or copied.
- (3) Indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.
- (4) Whether the information has been made public.

As of late 2018, no other state imposed these requirements. Businesses confronting a 50-state breach, however, need to account for these steps in addition to the tight time deadlines (and government reporting obligations<sup>20</sup>) imposed by several states.

Other states include certain express undertakings or make clear that notification is not required if the breach is unlikely to result in identity theft or other harm to consumers. **Colorado**, for example, obligates a covered entity that maintains, owns or licenses computerized data that includes personal information about a resident of Colorado, to “conduct in good

---

<sup>18</sup>Ala. Code § 8-38-4(a).

<sup>19</sup>Ala. Code § 8-38-4(b).

<sup>20</sup>See *infra* § 27.08[8].

faith a prompt investigation to determine the likelihood that personal information has been or will be misused” when it becomes aware that a security breach may have occurred, and thereafter requires that notice be provided to affected Colorado residents “unless the investigation determines that the misuse of information about a Colorado resident has not occurred and is not reasonably likely to occur.”<sup>21</sup> **Idaho** and **Nebraska** similarly require a reasonable and prompt investigation and notice if the investigation determines that the misuse of information about a state resident has occurred or is reasonably likely to occur.<sup>22</sup> **Kansas**<sup>23</sup> and **Utah**<sup>24</sup> impose a very similar obligation as Colorado, except that the prompt investigation required by Kansas and Utah law must also be “reasonable” and under Kansas law notice must be given as soon as possible “[i]f the investigation determines that the misuse of information has occurred or is reasonably likely to occur . . . .”<sup>25</sup>

**Maryland**’s statute was similar to the Kansas law (with some variation) but was amended in 2017 to provide that if, following a mandatory investigation, a business determines that the breach “creates a likelihood that personal information has been or will be misused,” the business must give notice “as soon as reasonably practicable but not later than 45 days after the business concludes” its investigation (or for a business that does not own or license the data, 45 days after

---

<sup>21</sup>Colo. Rev. Stat. § 6-1-716(2)(a).

<sup>22</sup>Idaho Code Ann. § 28-51-105; Neb. Rev. Stat. § 87-803(1). **Hawaii** defines a security breach in terms of where an “illegal use of . . . personal information has occurred, or is reasonably likely to occur and . . . creates a risk of harm to a person.” Haw. Rev. Stat. Ann. § 487N-1.

<sup>23</sup>Kan. Stat. Ann. § 50-7a02(a).

<sup>24</sup>Utah Code Ann. § 13-42-202(1).

<sup>25</sup>Under Kansas law, notice from a person or entity that maintains data to the owner or licensee must be given “following discovery of a breach, if the personal information was, or is reasonably believed to have been, accessed and acquired by an unauthorized person.” Kan. Stat. Ann. § 50-7a02(b) (emphasis added). The data owner, in turn, must conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has or will be misused. If the investigation determines that misuse has occurred or is reasonably likely to occur, notice must be provided “as soon as possible . . . in the most expedient time possible and without reasonable delay, consistent with the legitimate needs or law enforcement . . . and any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.” Kan. Stat. Ann. § 50-7a02(a).

being notified of the breach).<sup>26</sup>

**New Hampshire** law requires that when a person doing business in the state who owns or licenses computerized data that includes personal information, it “shall, when it becomes aware of a security breach, *promptly determine the likelihood that the information has been or will be misused.*”<sup>27</sup>

The **Arkansas** and **Louisiana** statutes contemplate a reasonable investigation.<sup>28</sup> **Iowa** and **Rhode Island** similarly require that notice be sent “after an appropriate investigation or after consultation with relevant federal, state, or local” law enforcement agencies.<sup>29</sup> **Alaska**’s law follows these other states but merely requires an appropriate investigation and notice to the Attorney General.<sup>30</sup>

Other states simply permit a delay to allow an evaluation of whether personal information has been compromised or to detect and correct the security problem or to determine sufficient contact information.<sup>31</sup> Indeed, the formulation used in California’s statute—“without unreasonable delay, consistent with the legitimate needs of law enforcement”—presupposes some delay for investigation by merely proscribing delays that are *unreasonable*.

Some allow—or even mandate—a further delay to aid law enforcement investigations. For example, **California** and **Kentucky** (for companies and individuals) require that a disclosure be made “in the most expedient time possible and

<sup>26</sup>See Md. Code Ann., Com. Law §§ 14-3504(b)(3), 14-3504(c)(2).

<sup>27</sup>31 N.H. Rev. Stat. Ann. § 359-C:20(I)(a) (emphasis added). Notice is required if misuse of the information occurred or if a determination cannot be reached. 31 N.H. Rev. Stat. Ann. § 359-C:20(I)(a).

<sup>28</sup>The statutes provide that “notification is not required if, after a reasonable investigation, the person or business determines that there is no reasonable likelihood of harm to consumers.” Ark. Code Ann. § 4-110-105(d); La. Stat. § 51:3074(G).

<sup>29</sup>Iowa Code Ann. § 715C.2(6); R.I. Gen. Laws § 11-49.2-4.

<sup>30</sup>Alaska Stat. § 45.48.010(c).

<sup>31</sup>For example, **North Carolina** law requires that notice be provided “without unreasonable delay, . . . 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). **Michigan** provides that a person or agency may delay providing notice if a delay is “necessary in order for the person or agency to take any measures necessary to determine the scope of the security breach and restore the reasonable integrity of the database.” Mich. Comp. Laws Ann. § 445.72(4).

without unreasonable delay, consistent with the legitimate needs of law enforcement . . . , or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.”<sup>32</sup> **Missouri’s** statute contains the same language except that the duty to provide notice is also modified as consistent with any measures necessary to determine sufficient contact information.<sup>33</sup>

Different rules, however, apply to contractors in Kentucky with respect to breaches obtained from state agencies. Kentucky’s breach notification statute for breaches involving government agencies and educational institutions<sup>34</sup> applies as well to *nonaffiliated third parties*, who are contractors who receive personal information from an agency.<sup>35</sup> A nonaffiliated third party generally is required to notify the agency from which it obtained access to personal information of a breach within 72 hours of discovery of the breach (unless delayed based on a notice from law enforcement).<sup>36</sup>

**Alaska, California, Kentucky,<sup>37</sup> Michigan, New Mexico,<sup>38</sup> New York, Pennsylvania, South Carolina, Tennessee, Washington** and other states as well as the **Virgin Islands** provide that notice *may* be delayed if a law enforcement agency determines that it will impede a criminal investigation (and in **Massachusetts** the law enforcement agency provides written notice of this fact to the person or agency intending to provide notice and to the State Attorney General,<sup>39</sup> while in **Pennsylvania** written notice referencing the specific code provision must be provided)<sup>40</sup> (or in Ohio, jeopardize homeland or national security, or in

<sup>32</sup>Cal. Civ. Code §§ 1798.29(a), 1798.82(a); Ky. Rev. Stat. Ann. § 365.732(2).

<sup>33</sup>Mo. Rev. Stat. § 407.1500.2(1)(c).

<sup>34</sup>See Ky. Rev. Stat. Ann. §§ 61.931 *et seq.*

<sup>35</sup>See Ky. Rev. Stat. Ann. § 61.931(5).

<sup>36</sup>See Ky. Rev. Stat. Ann. § 61.932.

<sup>37</sup>Ky. Rev. Stat. Ann. § 365.732(4). The Kentucky statute further provides that notification “shall be made promptly after the law enforcement agency determines that it will not compromise the investigation.” *Id.* Most other states that use the same language omit the word “promptly” from their laws.

<sup>38</sup>N.M. Stat. Ann. §§ 57-12C-6(B), 57-12C-9.

<sup>39</sup>Mass. Gen. L. Ann. ch. 93H, § 4.

<sup>40</sup>Pa. Stat. § 2304 (notification “may be delayed if a law enforcement agency determines and advises the entity in writing specifically referenc-

**Maryland** “impede a criminal investigation or jeopardize homeland or national security” provided that notice then be given as soon as reasonably practicable but not later than 30 days after law enforcement determines this risk has passed<sup>41</sup> (or to “determine the scope of the breach . . . , identify the individuals affected, or restore the integrity of the system.”)<sup>42</sup> or in **Guam, Michigan** or **West Virginia** (with the bracketed words added) or **Missouri** and **New Hampshire** (with reference to “civil investigation” deleted)<sup>43</sup> “impede a criminal or civil investigation or [jeopardize] homeland or national security”) and in **Illinois, Iowa** and **Oregon** if the law enforcement agency has made a written request that the notification be delayed,<sup>44</sup> but must be provided once the agency determines that it would not compromise the investigation (or in the case of **Kansas**<sup>45</sup> and **Nebraska**,<sup>46</sup> 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” or in West Virginia and (with immaterially different language) and Guam and Michigan simply “without unreasonable delay after the law-enforcement agency determines that notification will no longer impede the investigation or jeopardize national or homeland security.”). **Wyoming** provides that notice may be delayed if a law enforcement agency determines *in writing* that the notification may seriously impede a criminal investigation.<sup>47</sup> **Minnesota**, by contrast, provides that notification may be delayed “to a date certain” if a law enforcement agency “affirmatively determines that the notification will impede a criminal investigation.”<sup>48</sup>

Other states, such as **Alabama, Connecticut, Florida**

---

ing this section that the notification will impede a criminal or civil investigation. The notification . . . shall be made after the . . . agency determines that it will not compromise the investigation or national or homeland security.”).

<sup>41</sup>Md. Code Ann., Com. Law § 14-3504(d).

<sup>42</sup>Md. Code Ann., Com. Law § 14-3504(d)(1)(ii).

<sup>43</sup>Mo. Rev. Stat. § 407.1500.2(3); 31 N.H. Rev. Stat. Ann. § 359-C:20(II).

<sup>44</sup>See 815 Ill. Comp. Stat. Ann. §§ 530/10(b-5), 530/12(a-5); Iowa Code Ann. § 715C.2(3); Or. St. § 646A.604(3).

<sup>45</sup>Kan. Stat. Ann. § 50-7a02(c).

<sup>46</sup>Neb. Rev. Stat. § 87-803(4).

<sup>47</sup>Wyo. Stat. Ann. § 40-12-502(b) (emphasis added).

<sup>48</sup>Minn. Stat. Ann. § 325E.61(1)(c).

and **Mississippi**, provide that notice *shall* be delayed for a reasonable period of time if a law enforcement agency determines that the notification will impede a criminal investigation (or, in the case of Alabama and Mississippi, “a criminal investigation or national security”) and has requested that notice be delayed (which under Alabama law must be a written request).<sup>49</sup> **Hawaii** and **North Carolina** requires that notice be delayed if a law enforcement agency informs the business that notification may impede a criminal investigation or jeopardize national or homeland security, provided that such request is made in writing or the business documents such request contemporaneously in writing (including the name and agency of the officer making the request).<sup>50</sup> **Wisconsin** provides that a law enforcement agency may ask that notice not be made, to protect an investigation or homeland security, in which case an entity “may not provide notice of or publicize an unauthorized acquisition of personal information, except as authorized by the law enforcement agency that made the request.”<sup>51</sup>

**New Jersey** more specifically requires that the State Police be notified in advance of any disclosure to consumers and provides that notification shall be delayed if a law enforcement agency determines that the notification will impede a criminal or civil investigation and the agency has requested delay.<sup>52</sup> **Indiana**, by contrast, requires that any disclosures required in the event of a security breach by a person or private entity must be disclosed “without unreasonable delay,” and defines as reasonable a delay that is necessary to restore the integrity of the computer system, necessary to discover the scope of the breach, or made in response to a request from the attorney general or a law enforcement agency to delay disclosure because it will impede a criminal or civil investigation or jeopardize

---

<sup>49</sup>Ala. Code § 8-38-5(c); Conn. Gen. Stat. Ann. § 36a-701b(d); Fla. Stat. Ann. § 501.171(4)(a); Miss. Code Ann. § 75-24-29(5).

<sup>50</sup>Haw. Rev. Stat. Ann. § 487N-2(c); N.C. Gen. Stat. § 75-65(c). Upon communication by the agency that notice will no longer impede the investigation or jeopardize national security (or in the case of North Carolina, national security or homeland security), consumer notice must be provided “without unreasonable delay . . . .”

<sup>51</sup>Wis. Stat. Ann. § 134.98(5).

<sup>52</sup>N.J. Stat. Ann. § 56:8-163(c).

national security.<sup>53</sup> **Texas** provides that a person may delay providing notice at the request of a law enforcement agency that determines that the notification will impede a criminal investigation. Notice must be made “as soon as” the law enforcement agency determines that the notice will not compromise the investigation.<sup>54</sup> The statute in force in **Utah**,<sup>55</sup> like the original Texas statute, allows for delays for law enforcement or “as necessary to determine the scope of the breach and restore the reasonable integrity of the data system.”

As noted above, approximately six states require that any delay intended to avoid impeding a criminal investigation be based on a written request from law enforcement.<sup>56</sup> Other states do not require a written request to justify a delay, but it nonetheless would be prudent, if practicable, to obtain written evidence justifying any delay in providing notice to consumers in case of a later challenge by state regulators or in litigation. Where notice is delayed pursuant to a written request, the request may be revoked, at which time notice should be sent.<sup>57</sup>

An increasing minority of states have set outer time limits on when notice must be provided. **Colorado**<sup>58</sup> and **Florida**,<sup>59</sup>

<sup>53</sup>Ind. Code § 24-4.9-3-3.

<sup>54</sup>Tex. Bus. & Comm. Code § 521.053(d); Tex. Gov’t Code §§ 205.010, 2054.1125 (applying section 521.053(d) to state and local governments). Under the old law, in effect prior to Sept. 1, 2009, Texas allowed for delays for law enforcement or “as necessary to determine the scope of the breach and restore the reasonable integrity of the data system.” Tex. Bus. & Comm. Code § 48.103(b) (repealed).

<sup>55</sup>Utah Code Ann. § 13-42-202(2) (employing slightly different language).

<sup>56</sup>See Ala. Code § 8-35-5(c); Fla. Stat. Ann. § 501.171(4)(b); 815 Ill. Comp. Stat. Ann. §§ 530/10(b-5), 530/12(a-5); Iowa Code Ann. § 715C.2(3); Ky. Rev. Stat. Ann. § 61.933(3)(a); Or. St. § 646A.604(3).

<sup>57</sup>It is implicit in all statutes that require or permit notice to be delayed so as to not interfere with a criminal investigation, that at some point in time the need for delay would end and that at such time notice should be provided. Two states—Alabama and Florida—also make express provision for revocation by law enforcement of a written request to delay consumer notice, which also must be in writing. See Ala. Code § 8-35-5(c); Fla. Stat. Ann. § 501.171(4)(b).

<sup>58</sup>Colo. Rev. Stat. Ann. §§ 6-1-716(2)(a) (private entities), 24-73-103(2) (government agencies).

<sup>59</sup>Fla. Stat. Ann. § 501.171(4)(a). Florida requires that notice to

require notice within **30 days**, while **Alabama**,<sup>60</sup> **Arizona**,<sup>61</sup> **Delaware**,<sup>62</sup> **Maryland**,<sup>63</sup> **New Mexico**,<sup>64</sup> **Ohio**,<sup>65</sup> **Oregon**,<sup>66</sup> **Rhode Island**,<sup>67</sup> **Tennessee**,<sup>68</sup> **Vermont**,<sup>69</sup> **Washington**<sup>70</sup>

individuals be provided “as expeditiously as practicable and without unreasonable delay, taking into account the time necessary to allow the covered entity to determine the scope of the breach of security, to identify individuals affected by the breach, and to restore the reasonable integrity of the data system that was breached, but no later than 30 days after the determination of a breach or reason to believe a breach occurred” unless a delay is authorized by section 501.171(4)(b), if a federal, state, or local law enforcement agency determines that notice would interfere with a criminal investigation, or if pursuant to section 501.171(4)(b) the covered entity, after consulting with relevant federal, state or local law enforcement agencies, “reasonably determines that the breach has not and will not likely result in identity theft or any other financial harm to the individuals whose personal information has been accessed.” The 30-day notice period also may be extended by an additional 15 days if good cause for delay is shown in writing to the Florida Department of Legal Affairs within 30 days after determination of the breach or reason to believe a breach occurred.” Fla. Stat. Ann. § 501.171(3)(a).

<sup>60</sup>See Ala. Code §§ 8-38-4, 8-38-5(b). Subject to the investigation required by section 8-38-4 and the potential for delay set forth in section 8-38-5(c), section 8-38-5(b) requires notice within 45 days “of the covered entity’s receipt of notice from a third party agent that a breach has occurred or upon the covered entity’s determination that a breach has occurred and is reasonably likely to cause substantial harm to the individuals to whom the information relates.” *Id.* § 8-38-5(b).

<sup>61</sup>See Ariz. Rev. Stat. Ann. § 18-552(B).

<sup>62</sup>Del. Code Ann. tit. 6, §§ 12B-102(c).

<sup>63</sup>Md. Code Ann., Com. Law §§ 14-3504(b)(3), 14-3504(c)(2).

<sup>64</sup>N.M. Stat. Ann. §§ 57-12C-6(B), 57-12C-6(C). The 45 calendar day deadline, which runs from the date of discovery of the breach, is subject to the caveat that notice is not required if, after an appropriate investigation, the person otherwise required to provide notice “determines that the security breach does not give rise to a significant risk of identity theft or fraud.” *Id.* The 45 day deadline also may be avoided if a law enforcement agency determines that the notification will impede a criminal investigation or “as necessary to determine the scope of the security breach and restore the integrity, security and confidentiality of the data system.” *Id.* § 57-12C-9.

<sup>65</sup>Ohio Rev. Code Ann. §§ 1347.12(b)(2), 1349.19(B)(2). Ohio requires that notice be provided in the most expedient time possible but not later than forty-five (45) days from notice or discovery of a breach unless provisions governing delay for law enforcement or investigation apply.

<sup>66</sup>Or. Rev. Stat. Ann. § 646A.604(3).

<sup>67</sup>Rhode Island law requires notice within forty-five (45) days after confirmation of a breach and the ability to ascertain the information required to fulfill the notice requirements of the amended statute, unless

and **Wisconsin**<sup>71</sup> impose an outside maximum time, within which notice must be made, of **forty-five (45) days** (although, in the case of Florida, the thirty (30) day time limit may be extended by an additional 15 days if good cause for the delay is provided in writing to the Department of Legal Affairs within the initial thirty day period).<sup>72</sup> **Delaware** provides for notice “without unreasonable delay but not later than **60 days** after determination of the breach . . .,” except if a shorter time is required by federal law or if a law enforcement agency determines that the notice will impede a crimi-

---

a delay is sought by law enforcement. *See* R.I. Gen. Laws §§ 11-49.3-4(a)(2), 11-49.3-4(b); *see generally infra* § 27.09[43] (providing the text of the law).

<sup>68</sup>Tenn. Code Ann. § 47-18-2107(c). Tennessee requires that disclosure of a breach be made immediately, but no later than forty-five (45) days from the discovery or notification of the breach, unless a longer time is required due to the legitimate needs of law enforcement.

<sup>69</sup>Vt. Stat. Ann. tit. 9, § 2435(b)(1). Vermont requires that notice be provided “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 [as provided for in sections 2435(b)(3) and 2435(b)(4)] . . . 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.” *Id.* While this framework allows for additional time when needed, a preliminary description of the breach along with the date of the breach and date of discovery must be provided to the Attorney General in many cases within fourteen days discovery of the breach or provision of notice to consumers, whichever is sooner. *Id.* § 2435(b)(3)(A)(i); *see generally infra* §§ 27.08[8] (notice to state agencies); 27.09[49] (reprinting Vt. Stat. Ann. tit. 9, § 2435).

<sup>70</sup>Wash. Rev. Code Ann. § 19.255.010(16); Wash. Rev. Code Ann. § 42.56.590(15).

<sup>71</sup>Wisconsin provides that notice must be provided “within a reasonable time, not to exceed forty-five (45) days after the entity learns of the acquisition of personal information” and further elaborates that a determination of reasonableness in this context “shall include consideration of the number of notices that an entity must provide and the methods of communication available to the entity.” Wis. Stat. Ann. § 134.98(3)(a).

An entity that stores but does not own or license personal information must notify the owner or licensor under Wisconsin law “as soon as practicable.” Wis. Stat. Ann. § 134.98(2)(bm).

<sup>72</sup>Fla. Stat. Ann. § 501.171(3)(a) (stating that a “covered entity may receive 15 additional days to provide notice as required in subsection (4) if good cause for delay is provided in writing to the department within 30 days after determination of the breach or reason to believe a breach occurred”).

nal investigation and requests that notice be delayed),<sup>73</sup> **South Dakota** likewise requires notification to consumers not later than **60 days** from discovery or notice (except where notice would impede a criminal investigation, in which case notice must be made not later than 30 days after the law enforcement agency determines that notification will not compromise the criminal investigation),<sup>74</sup> and **Connecticut**<sup>75</sup> sets a **ninety (90) day** limit for notifying state residents, unless a shorter time is required by federal law. These time periods typically run from notice or discovery of a breach (or, under the Florida statute, after the determination of a breach or reason to believe a breach occurred, or under Rhode Island law, after confirmation of a breach and the ability to ascertain the information required to fulfill the notice requirements of the amended statute, or pursuant to Maryland's statute, after a business that owns or licenses the data, concludes its investigation, or 45 days from the time a business that does not own or license the data receives notice).

The time for sending notice under these statutes is subject to provisions governing delay for law enforcement (and, in the case of Ohio, investigation, or in the case of Florida, a determination, made following an investigation and in consultation with relevant federal, state or local enforcement agencies that “the breach has not and will not likely result in identity theft or any other financial harm to the individuals whose personal information has been accessed.”<sup>76</sup>). In multiple states, including **Alabama, Arizona, Florida, New Mexico, Rhode Island, Tennessee** and **Wisconsin**, these considerations could extend the time to give notice beyond the maximum number of days prescribed (although under Tennessee's statute notice must then be sent no later than 45 days after the law enforcement agency determines that notification will not compromise the investigation).<sup>77</sup> In **Ohio**, by contrast, they provide grounds for delay up to but

---

<sup>73</sup>Del. Code Ann. tit. 6, §§ 12B-102(c) (emphasis added).

<sup>74</sup>S.D. Codified Laws §§ 22-40-20, 22-40-21.

<sup>75</sup>Conn. Gen. Stat. Ann. § 36a-701b(b)(1).

<sup>76</sup>Fla. Stat. Ann. § 501.171(4)(b). Notice must be delayed if a federal, state or local law enforcement agency determines that notice to individuals would interfere with a criminal investigation, upon the written request of the law enforcement agency for a specified period that the law enforcement agency determines is reasonably necessary. *Id.*

<sup>77</sup>Tenn. Code Ann. § 47-18-2107(d).

not beyond the forty-five-day limit.<sup>78</sup> While most statutes do not set a hard deadline, it is likely that regulators in many states would consider even forty-five days too long given that notice is usually most effective at preventing identity theft or other adverse consequences of a security breach the sooner it is received and acted upon by consumers.

**Florida** law also provides that persons who maintain computerized data on behalf of others must provide notice to the owner or licensee of such data “as expeditiously as practicable” but in any case not later than ten days following the determination of the breach or reason to believe that the breach occurred.<sup>79</sup>

**Delaware** makes provision for notice outside of the 60 day period ordinarily required if, through reasonable diligence, it could not have been determined that a person’s information was included in a breach. If so, then notice generally must be sent “as soon as practicable after the determination that the breach of security included the personal information” of such a person.<sup>80</sup>

**New Mexico** further provides that notwithstanding other provisions of the security breach notification law that would point to an obligation to provide notice, notice is not required if, after an appropriate investigation, the person otherwise required to provide notice “determines that the security breach does not give rise to a significant risk of identity theft or fraud.”<sup>81</sup>

**Missouri** does not impose an outside limit for sending notice but does provide that once an investigation has been completed, notice to consumers must be sent no longer than seven business days after a law enforcement agency determines that the notification will not compromise a criminal investigation.<sup>82</sup>

While **Minnesota**, like California and many other states, merely requires notice “following discovery or notification” in

---

<sup>78</sup>The basis for this conclusion is set forth in the preceding footnotes.

<sup>79</sup>Fla. Stat. Ann. § 501.171(6)(a). A third party required to provide this notice must supply the covered entity with all information that it would need to provide notice to consumers and the Department of Legal Affairs. *Id.*

<sup>80</sup>Del. Code Ann. tit. 6, §§ 12B-102(c)(3).

<sup>81</sup>N.M. Stat. Ann. §§ 57-12C-6(B), 57-12C-6(C).

<sup>82</sup>Me. Rev. Stat. Ann. tit. 10, § 1348(3).

“the most expedient time possible and without unreasonable delay, . . .” it also sets a time limit on how quickly consumer reporting agencies must be notified, as discussed in greater detail below in section 27.08[7].

**Puerto Rico** effectively imposes the most rigid time line of any U.S. jurisdiction. While notice need only be provided to clients “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” the statute also requires that notice be given to Puerto Rico’s Department of Consumer Affairs within “a non-extendable term of ten (10) days after the violation” and directs the Department to make a public announcement of the breach within twenty-four hours after having received this information.<sup>83</sup> As a practical matter, this means that from a public relations standpoint notice to consumers in Puerto Rico should be made within eleven days of detection of a breach (and preferably ten) to precede a public announcement by the Department of Consumer Affairs. Whether notice to customers is sent within that time period or not, the fact of the breach potentially will become a matter of public record within eleven days.

The requirement noted above in **Illinois, Iowa and Oregon** that notice to consumers not be sent until the applicable law enforcement agency determines that disclosure will not compromise a criminal investigation and notifies the affected person of this fact in writing, may be problematic because of the requirement in Florida, Ohio and Puerto Rico that notice to consumers (or in the case of Puerto Rico, to the Department of Consumer Affairs) be sent within a fixed number of days without exception (or, in the case of Florida, unless a written waiver is obtained).<sup>84</sup> The requirement may also be difficult to comply with if a law enforcement agency

---

<sup>83</sup>10 L.P.R. Ann. §§ 4052, 4051(b).

<sup>84</sup>Where approval to send notice to consumers cannot be obtained within forty-five (45) days of notice or discovery of the breach, the requirements of **Illinois, Iowa and Oregon** laws could compel a person or individual to breach its obligation to provide notice in most instances within thirty days to residents of **Florida** and forty-five days to residents of **Ohio**, assuming that the breach involves residents of these states. The delay would not constitute a breach of the **Tennessee, Vermont, Wisconsin and Washington** security breach statutes, whose forty-five-day deadlines are made subject to the needs of law enforcement. The obliga-

is unwilling to provide written notice. While law enforcement agencies are usually not shy about asking that notice be deferred when appropriate, it is sometimes difficult to get someone to sign off in writing that a criminal investigation will not be jeopardized if notice is sent.

### 27.08[5] Methods of Notification

If a disclosure must be made, statutes generally provide alternative means for providing notice, such as written notice; electronic notice, if the notice is consistent with the provisions of the federal eSIGN statute<sup>1</sup> (or simply an “electronic notice” in **Guam**, **Oklahoma** (for individuals and entities) and **Virginia**<sup>2</sup> or, in **Puerto Rico**, pursuant to the Digital

tion to provide notice within forty-five days under **Rhode Island** law runs from “after confirmation of the breach and the ability to ascertain the information required to fulfill the notice requirements” set forth in the statute. Both **Vermont** and **Washington** further provide that the forty-five day deadline can be extended as needed to determine the scope of the breach and restore the reasonable integrity of the data system.

The notice required under **Puerto Rico**’s statute would not necessarily constitute a breach of Illinois, Iowa or Oregon laws that focus on the timing of notice to consumers, but because it would result in public disclosure of the breach it would certainly undermine the purpose of these statutes to keep the breach confidential pending a criminal investigation.

#### [Section 27.08[5]]

<sup>1</sup>15 U.S.C.A. §§ 7001 *et seq.*; *see generally supra* § 15.02 (analyzing the eSIGN statute). **Nebraska** incorporates the provisions of the eSIGN statute as they existed on Jan. 1, 2006. Neb. Rev. Stat. § 87-802(3)(c). **New York** does not reference eSIGN, but instead allows “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 notice is kept . . . .” N.Y. Gen. Bus. L. § 899-aa(5). New York law further provides that a person may not be required to consent to accept such notice as a condition of establishing any business relationship or engaging in any transaction. N.Y. Gen. Bus. L. § 899-aa(5).

<sup>2</sup>9 Guam Code Ann. § 48.20(g)(3); Okla. Stat. Ann. tit. 24, § 162(7)(c); Va. Code Ann. § 18.2-186.6(A). The term *electronic notice* is neither defined in the security breach notification statute nor in other Virginia statutes but presumably means something different from e-mail notice, which is permitted under the security breach statute only in conjunction with conspicuous posting on website and notice to major statewide media where substitute notice is authorized. *See* Va. Code Ann. § 18.2-186.6(A). Based on other Virginia statutes it may be inferred that the legislature intended to permit electronic notice in cases where consent was obtained from recipients to obtain notice by electronic means, which would also be consistent with the mechanism for providing electronic notice under the federal eSIGN statute which is referenced in place of “electronic notice” in

Signatures Act<sup>3</sup>); or substitute notice (as described below).

Some states also allow notice by telephone<sup>4</sup> or fax,<sup>5</sup> although these methods could not be used on a nationwide

---

the security breach notification statutes of multiple other states.

The term likewise is not defined in Oklahoma's notification statute for breaches by individuals and entities, which was adopted in 2008 and based on Virginia's law. Oklahoma's earlier notification statute (Okla. Stat. Ann. tit. 74, § 3113.1), enacted in 2006, applies to state agencies and was modeled on the original California statute.

Guam's notification statute was modeled on Virginia's.

<sup>3</sup>10 L.P.R. Ann. § 4053(1). The reference to Digital Signatures Act was probably intended to refer to Puerto Rico's Electronic Signatures Act, which is codified at 3 L.P.R. Ann. §§ 8701 to 8707b; *see generally supra* § 15.02 (analyzing eSIGN and state digital signature laws).

<sup>4</sup>For example, **Arizona, Colorado, Connecticut, Delaware, Guam, Georgia, Hawaii, Idaho, Maryland, Michigan, Mississippi, Missouri, Montana, Nebraska, New Hampshire, New York, North Carolina, Ohio, Oklahoma** (for breaches involving individuals and entities, not government agencies); **Oregon, Pennsylvania, South Carolina, Utah, Vermont, Virginia** and **West Virginia** allow notice by telephone. A number of states impose conditions on telephone notice, however.

Utah authorizes notice by telephone, "including through the use of automatic dialing technology not prohibited by other law . . . ." Utah Code Ann. § 13-42-202(5)(a)(iii).

Michigan, by contrast, allows notice by phone, if not otherwise prohibited by state or federal law, provided (1) the notice is not given in whole or in part by use of a recorded message; and (2) the recipient has expressly consented to receive notice by telephone, or if the recipient has not expressly consented to receive notice by telephone, the person or agency also provides written notice or, if permitted, email notice, if the notice by telephone does not result in a live conversation between the individual representing the person or agency and the recipient within three business days after the initial attempt to provide telephonic notice. Mich. Comp. Laws Ann. § 445.72(5)(c).

Arizona and Vermont allow telephonic notice provided that telephonic contact is made directly with each affected consumer, and the telephonic contact is not through a prerecorded message. Ariz. Rev. Stat. Ann. § 18-552(F)(3); Vt. Stat. Ann. tit. 9, § 2435(b)(6)(A)(iii). Hawaii, Missouri, and North Carolina similarly permit telephonic notice provided contact is made directly with the affected persons. Haw. Rev. Stat. Ann. § 487N-2(e)(3); Mo. Ann. Stat. § 407.1500(6)(c); N.C. Gen. Stat. Ann. § 75-65(e)(3). Although not express like the Arizona and Vermont laws, the provision employed by Hawaii, Missouri, and North Carolina implicitly prohibits use of a prerecorded message.

Maryland permits notice by telephone provided it is made to "the most recent telephone number of the individual in the records of the business . . . ." Md. Code Ann. Com. Law § 14-3504(e)(3); *see also* Md. Code Ann. State Gov't § 10-1305(e)(3) (applying a similar rule to state agencies).

basis.

**New York** further imposes record-keeping requirements if electronic or telephone notice is used.<sup>6</sup>

Notice by email is *not* authorized in most states unless in compliance with the federal eSIGN statute (or equivalent provisions), undertaken pursuant to an information security policy<sup>7</sup> (so long as consistent with the timing requirements of the statute and in **Indiana**<sup>8</sup> if the plan provides for notice to be sent to state residents, the attorney general and owner's primary regulator), or pursuant to a private contract in **Ohio**,<sup>9</sup> or as one of three forms of notice that each must be provided to qualify as substitute notice under applicable statutes (or two out of three, in the case of **Guam**).

---

New Hampshire allows notice by telephone "provided that a log of each such notification is kept by the person or business who notifies the affected persons." 31 N.H. Rev. Stat. Ann. § 359-C:20(III)(c).

Pennsylvania authorizes notice by telephone "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 Internet website to visit for further information or assistance." 73 Pa. Stat. Ann. § 2302.

The laws governing lawful use of automated dialing technologies and prerecorded calls are set forth in chapter 29 (in section 29.16).

<sup>5</sup>See, e.g., Ind. Code § 24-4.9-3-4(a)(3).

<sup>6</sup>N.Y. Gen. Bus. L. § 899-aa(5). A log of such notice must be kept.

<sup>7</sup>Most notification statutes create an incentive for companies to adopt security compliance programs in order to be able to notify consumers by email in the event of a security breach. **Arizona** affirmatively requires various municipal agencies, including courts and sheriff departments, to create and maintain information security policies that include notification procedures. See Ariz. Rev. Stat. § 18-552(K). Massachusetts also has enacted a separate information security statute. See *supra* § 27.04[6][E].

By contrast, **Hawaii** and **Puerto Rico** do not make provision for email service pursuant to an information security policy. In Hawaii, notice by email would only be permitted pursuant to eSIGN or where substitute notice is allowed.

<sup>8</sup>Ind. Code § 24-4.9-3-4(c)(6).

<sup>9</sup>Ohio's security breach notification statute provides that disclosure "may be made pursuant to any provision of a contract entered into by the person with another person prior to the date of the breach . . . 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 Ann. § 1349.19(B)(1). This provision appears to allow for notice by email only to the extent otherwise permitted under Ohio law, as discussed below.

Email notice is permissible, however, without qualification, for residents of **Alabama**,<sup>10</sup> **Wyoming**<sup>11</sup> and **Florida**<sup>12</sup> (and, indeed, generally *must* be sent by either U.S. mail or email to residents of Alabama and Florida) and, subject to express conditions, in the following states:

- **Alaska**,<sup>13</sup> **Arizona**,<sup>14</sup> **Colorado**,<sup>15</sup> **Delaware**,<sup>16</sup> **Minnesota**,<sup>17</sup> **Mississippi**,<sup>18</sup> **New Hampshire**,<sup>19</sup> **Utah**<sup>20</sup> and **Vermont**<sup>21</sup> (if the person’s “primary method” or “primary means” of communication with the resident or consumer or entity (depending on the terminology used in the particular statute) is “by electronic means”), with a similar provision in effect in **New Mexico** (“if the person required to make the notification primarily communicates with the New Mexico resident by electronic means . . .”),<sup>22</sup> **Ohio** (“if the person’s primary method of communication with the resident to whom the disclosure must be made is by electronic means,”<sup>23</sup> for individuals and companies, or “if the state agency’s or agency of a political subdivision’s primary method of communication with the resident to whom disclosure must be made is by electronic means”)<sup>24</sup> and **Oregon** (“if the person customarily communicates with the consumer electronically . . .”),<sup>25</sup>

---

<sup>10</sup>Ala. Code § 8-38-5(d).

<sup>11</sup>Wyo. Stat. Ann. § 40-12-502(d)(ii).

<sup>12</sup>See Fla. Stat. Ann. § 501.171(4)(d).

<sup>13</sup>Alaska Stat. § 45.48.030.

<sup>14</sup>Ariz. Rev. Stat. Ann. § 18-552(D)(2).

<sup>15</sup>Colo. Rev. Stat. Ann. § 6-1-716(1)(f)(III).

<sup>16</sup>Del. Code Ann. tit. 6, § 12B-101(3)(c).

<sup>17</sup>Minn. Stat. Ann. § 325E.61(g)(2).

<sup>18</sup>Miss. Code Ann. § 75-24-29(6).

<sup>19</sup>N.H. Rev. Stat. § 359-C:20(III)(b).

<sup>20</sup>Utah Code Ann. § 13-42-202(5)(a)(ii).

<sup>21</sup>Vt. Stat. Ann. tit. 9, § 2435(b)(6)(A)(ii).

<sup>22</sup>N.M. Stat. Ann. § 57-12C-6(D)(2).

<sup>23</sup>Ohio Rev. Code Ann. § 1347.19(E).

<sup>24</sup>Ohio Rev. Code Ann. § 1347.12(B)(2).

<sup>25</sup>Or. Rev. Stat. Ann. § 646A.604(4)(b).

- **Indiana** (if the individual has provided the state agency with his or her email address);<sup>26</sup>
- **Maryland** (if “[t]he business conducts its business primarily through Internet account transactions or the Internet” or the individual expressly consented to receive electronic notice);<sup>27</sup>
- **Michigan** (if the same requirements as those imposed under Maryland law apply and the person or agency “has an existing business relationship with the recipient that includes periodic electronic mail communications and based on those communications the person or agency reasonably believes that it has the recipient’s current email address”);<sup>28</sup>
- **Pennsylvania** (“if a prior business relationship exists and the person or entity has a valid email address for the individual.”).<sup>29</sup> and

Notice by email may be permitted under eSIGN or pursuant to **Alaska, New York, Puerto Rico** and potentially **Oklahoma** and **Virginia** law if express consent to receive such notice is provided on a voluntary basis.<sup>30</sup> As noted above, some, but not all states allow companies or individuals to provide alternative notice pursuant to their own information security policies.<sup>31</sup> State statutes therefore create an incentive for companies to plan ahead and either obtain consent for electronic communications or adopt a security policy. As a practical matter, however, few businesses do so.

While email, where available, is usually the cheapest method of providing notice, it is not always the most desirable. Among other things, email notices may be forwarded to third parties, transmitted over the Internet, posted on blogs and otherwise easily, quickly and inexpensively disseminated to generate negative publicity.

Substitute notice alternatively may be permissible depend-

---

<sup>26</sup>Ind. Code § 4-1-11-8; 24-4.9-3-4(a)(4).

<sup>27</sup>Md. Code Ann., Com. Law § 14-3504(e)(2).

<sup>28</sup>Mich. Comp. Laws Ann. § 445.72(5)(b).

<sup>29</sup>73 Penn. Stat. Ann. § 2302.

<sup>30</sup>The requirements under Oklahoma, New York, Puerto Rico and Virginia law are addressed in previous footnotes in this section, following the first annotated reference to eSIGN. As discussed earlier, it is unclear whether consent is required under Virginia law.

<sup>31</sup>See *supra* § 27.11.

ing on the size of the breach (or in some cases excessive cost or lack of sufficient contact information). Where permitted, substitute notice generally must be provided by (i) email (when the person or business has an email address for an intended recipient, in states where email is not otherwise a permitted way to send regular notice), (ii) conspicuous posting on the person or business's website (if one is maintained) and<sup>32</sup> (iii) notification to major statewide media (defined in some statutes, such as those in force in **Connecticut**<sup>33</sup> and **Mississippi**, to include newspapers, radio and television, subject to other limitations in **Ohio**;<sup>34</sup> or more specifically as "major statewide and regional media" in **Vermont**,<sup>35</sup> "local and, if applicable, national media" in the **District of Columbia**,<sup>36</sup> "a newspaper of general circulation" or on a website in **Utah**,<sup>37</sup> and for obvious reasons "major territory-

---

<sup>32</sup>All three methods generally must be used for substitute notice to be effective. **Montana**, however, provides for substitute notice by email when the person or business has an electronic mail address for intended recipients and conspicuous posting or notice to applicable statewide or local media. See Mont. Code Ann. § 30-14-1704(5)(b). **Florida**, which unlike most states, typically requires notice to consumers to be sent by mail delivery or email, provides for substitute notice, where the conditions for substitute notice have been met, by (1) "conspicuous notice on the Internet website of the covered entity if the covered entity maintains a website" and (2) notice "in print and to broadcast media, including major media in urban and rural areas where the affected individuals reside." Fla. Stat. Ann. § 501.171(4)(f).

**California** requires that the notice be posted for a minimum of 30 days and defines *conspicuous posting* on a website to mean "providing a link to the notice on the home page or first significant page after entering the Internet Web site that is in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks that call attention to the link."

<sup>33</sup>Conn. Gen. Stat. Ann. § 36a-701b(e).

<sup>34</sup>Notification to major media outlets is allowed under Ohio law "to the extent that the cumulative total of the readership, viewing audience, or listening audience of all of the outlets so notified equals or exceeds 75% of the population" of the state. Ohio Rev. Code §§ 1347.12(E)(4)(c) (state agencies), 1347.19(E)(4)(c) (private businesses).

<sup>35</sup>Vt. Stat. Ann. tit. 9, § 2435(b)(6)(B)(ii).

<sup>36</sup>D.C. Code § 28-3851(2)(C)(ii)(III).

<sup>37</sup>See Utah Code Ann. § 13-42-202(5)(a)(iv); see also Utah Code Ann. § 45-1-101 (setting forth the requirement for Web publication in lieu of or in addition to newspaper publication).

wide media” in the **Virgin Islands**),<sup>38</sup> or in **Illinois** major statewide media “or, if the breach impacts residents in one geographic area, to prominent local media in areas where affected individuals are likely to reside if such notice is reasonably calculated to give actual notice to persons whom notice is required . . . ,”<sup>39</sup> and in the case of **Michigan**, the statewide media notice must include a telephone number or website address that a person may use to obtain additional assistance and information. Pursuant to 2011 and 2013 amendments, **California** also requires that substitute notice, when provided by an agency, be sent to the Office of Information Security within the State Department of Technology.<sup>40</sup> **New Mexico** also requires that substitute service be made on the Office of the Attorney General.<sup>41</sup>

Substitute notice may be authorized if the person or business demonstrates that:

- the cost of providing notice would exceed some threshold dollar amount (**\$250,000** under Arkansas, California, Colorado, Connecticut, Florida, Illinois, Indiana, Iowa, Kentucky, Louisiana, Massachusetts, Michigan, Minnesota, Montana, Nevada, New Jersey, New York, North Carolina, Ohio, Oklahoma (for breaches involving state agencies), South Carolina, South Dakota, Tennessee, Texas and Washington law; **\$150,000** under the statutes in force in Alaska and Missouri; **\$100,000** under the laws of Hawaii, Kansas, Maryland, New Mexico, Pennsylvania and the U.S. Virgin Islands; **\$75,000** under Delaware and Nebraska law; **\$50,000** under Arizona, District of Columbia, Georgia, Oklahoma (for individuals or entities), Virginia and West Virginia law; **\$25,000** under Idaho and Rhode Island law; **\$10,000** under Guam’s statute; or **\$5,000** under Maine, Mississippi, New Hampshire and Vermont law),
- the affected class of persons to be notified<sup>42</sup> exceeds some number (**500,000** in Arkansas, California, Con-

<sup>38</sup>V.I. Code Ann. tit. 14, §§ 2208(I)(3)(C) (agencies), 2209(I)(3)(C) (persons and businesses).

<sup>39</sup>815 Ill. Comp. Stat. Ann. 530/10(c)(3).

<sup>40</sup>Cal. Civ. Code §§ 1798.82(j)(3)(C) (persons and businesses), 1798.29(i)(3)(C) (state agencies).

<sup>41</sup>N.M. Stat. Ann. § 57-12C-6(E)(3).

<sup>42</sup>Most (but not all) statutes focus on the total number of persons who

necticut, Florida, Illinois, Indiana, Kentucky, Louisiana, Massachusetts, Michigan, Minnesota, Montana, Nevada, New Jersey, New York, North Carolina, Ohio, Oklahoma (for breaches involving state agencies), South Carolina, South Dakota, Tennessee, Texas and Washington; **300,000** in Alaska; **350,000** in Iowa; **250,000** in Colorado; **200,000** in Hawaii; **175,000** in Maryland and Pennsylvania; **150,000** under Alaska and Missouri law; **100,000** in Arizona, Delaware, the District of Columbia, Georgia, Nebraska, Oklahoma (for individuals and entities), Virginia and West Virginia; **50,000** in Idaho, New Mexico, Rhode Island and the U.S. Virgin Islands; **5,000** in Guam, Kansas, Mississippi and Vermont; or **1,000** in Maine and New Hampshire) or

- the person or business does not have sufficient contact information to provide notice in the manner generally prescribed (or in the case of Missouri, sufficient contact information or consent, or if the person is unable to identify particular affected consumers, but only for those unidentified consumers).

**Wyoming**, which generally permits notice by email, provides for substitute notice by conspicuous posting on the Internet, Web or similar proprietary or common carrier electronic system sites and by notification to major statewide media (which must include a toll-free number where an individual can learn if his or her personal data is included in the security breach) if a person can demonstrate that (a) the cost of providing notice would exceed \$10,000 for Wyoming based persons or businesses and \$250,000 for all other businesses operating but not based in Wyoming; or (b) the affected class of people to be notified exceeds 10,000 for Wyoming-based persons or businesses and 500,000 for all other businesses operating but not based in Wyoming; or (c) the person does

---

would receive notice, rather than the number of people who would receive notice within a given state, which makes sense given that substitute notice is intended to provide an alternative mechanism to comply with security breach notification statutes when the class of recipients is so large that it would impose undue costs or other hardship on the party required to give notice. Virginia, for example, provides for substitute service based on the total number of Virginia residents to be sent notice. *See* Va. Code Ann. § 18.2-186.6(A). Puerto Rico's statute similarly refers to the number of people required to receive notice under the statute, which by its terms applies to residents of Puerto Rico.

not have sufficient contact information.<sup>43</sup>

**Alabama**, which ordinarily requires notice by U.S. mail or email, permits substituted service (in the form of a conspicuous notice on a covered entity's website for 30 days *and* notice in print and broadcast media, including major media in urban and rural areas where the affected individuals reside) if "direct notice is not feasible" due to excessive cost (defined as either "[e]xcessive cost to the covered entity relative to the resources of the covered entity" or \$500,000), or the "lack of sufficient contact information for the individual required to be notified . . .," or if there are more than 100,000 people affected by the breach.<sup>44</sup> **Florida**, which also ordinarily requires notice by U.S. mail or email, provides for similar substituted service as Alabama (without specifying the 30 day time period for website notice and without the excessive cost provision) if notice would cost \$250,000 or involve more than 500,000 people.<sup>45</sup>

**Nebraska** and **Ohio** provide for a second form of substitute notice where an individual, commercial entity or (in Ohio only) a state agency can demonstrate that it has ten or fewer employees and that the cost of providing notice would exceed \$10,000. If applicable, both states allow for notice to be effectuated through a quarter-page or larger paid advertisement appearing at least weekly for three consecutive weeks in a local newspaper that is distributed in the geographic area in which the state agency or agency of a political subdivision is located, by conspicuous posting on the agency's website (if it maintains one), and notification to major media outlets in the geographic area in which the agency is located.<sup>46</sup> Nebraska also requires that notice be provided by email if the person or entity has email addresses for the members of the affected class of Nebraska residents.<sup>47</sup>

**Michigan** likewise provides special alternative notice procedures for public utilities that send monthly billing or account statements to the postal addresses of their

---

<sup>43</sup>Wyo. Stat. Ann. § 40-12-502(d)(iii)(B).

<sup>44</sup>See Ala. Code § 8-38-59(e).

<sup>45</sup>See Fla. Stat. Ann. § 501.171(4)(d).

<sup>46</sup>Ohio Rev. Code §§ 1347.12(E)(5), 1347.19(E)(5).

<sup>47</sup>Neb. Rev. Stat. § 87-802(4)(e).

customers.<sup>48</sup>

**Puerto Rico** does not authorize the three basic means of providing substitute notice found in most statutes (email, posting on a website and notification to major media), instead providing that where substitute notice is permitted it must be provided by (1) prominent display of an announcement on an entity's web page, if any, and in "any informative flier published and sent through mailing lists both postal and electronic," and (2) "a communication . . . to the media informing of the situation and providing information as to how to contact the entity to allow for better follow-up" and "[w]hen 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 toward that sector."<sup>49</sup> Substitute notice is permitted in Puerto Rico when the cost of notice is "excessively onerous due to the number of people affected, the difficulty in locating all persons or to the economic situation of the enterprise or entity;" or whenever the cost of notice exceeds \$100,000 or the number of persons receiving notice exceeds 100,000.

Unlike most other states, **Wisconsin** merely requires entities obligated to do so to make "reasonable efforts"<sup>50</sup> to provide notice, which must be made "by mail or by a method the entity has previously employed to communicate with the subject of the personal information."<sup>51</sup> However, if an entity cannot "with reasonable diligence" determine a mailing address, and if it has not previously communicated with the affected person, the entity must provide notice "by a method reasonably calculated to provide actual notice to the subject of the personal information."<sup>52</sup> Depending on the circumstances, this presumably could include email, as well as other forms of substitute notice permitted under various state statutes analyzed in this sub-section.

### 27.08[6] The Content and Required Text of Consumer Notices

Most statutes still do not expressly specify the exact contents of what must be included in a notice to consumers,

---

<sup>48</sup>See Mich. Comp. Laws Ann. § 445.72(11).

<sup>49</sup>10 L.P.R. Ann. § 4053(2).

<sup>50</sup>Wis. Stat. Ann. § 134.98(2).

<sup>51</sup>Wis. Stat. Ann. § 134.98(3)(b).

<sup>52</sup>Wis. Stat. Ann. § 134.98(3)(b).

which allows businesses (and, where applicable, government agencies) to craft notices best suited to their own corporate culture and the sophistication of their consumers. An increasing number of states, however, including **California, Connecticut, Hawaii, Michigan, New Mexico, North Carolina, Rhode Island, Vermont, Virginia, Washington** and **Wyoming**, require that consumers be told (or not told) specific details about the breach and given notice of the things they may do to protect themselves against identity theft, such as contacting credit bureaus or placing security freezes<sup>1</sup> on their credit reports, and/or that notices be written in a specific way or contain particular language. A number also mandate clear and conspicuous notice or, in the case of **California** and **Washington**, the use of plain

---

[Section 27.08[6]]

<sup>1</sup>*See, e.g.*, Mass. Gen. L. Ann. ch. 93H, § 3(b); Conn. Gen. Stat. Ann. § 36a-701b(2)(B) (security freeze and notice of identity theft prevention and/or mitigation services); Del. Code Ann. tit. 6, § 12B-102(e) (security freeze and notice of identity theft prevention and/or mitigation services); W. Va. Code § 46A-2A-102(d) (right to place a fraud alert or security freeze); 815 Ill. Comp. Stat. Ann. 530/10(a) (disclosure that the recipient of the communication may obtain information from consumer reporting agencies or the FTC about fraud alerts and credit freezes), 530/12(a) (same disclosure, but required of state agencies).

Virtually all states mandate that notice of a consumer's right to place a credit freeze on his or her account be provided whenever a consumer credit reporting agency is required to give notice under the Fair Credit Reporting Agency. *See, e.g.*, Alaska Stat. § 45.48.170; Ga. Code Ann. § 10-1-915.

Others, such as **Oregon** and **Wyoming**, provide that a consumer reporting agency may not charge the victim of identity theft or who has filed a police report about a theft of data for a security freeze (but may otherwise charge no more than \$10 for the service). Or. Rev. Stat. Ann. § 646A.610; Wyo. Stat. Ann. § 40-12-506. **North Carolina** similarly provides that no fee may be charged for requests made electronically or to persons over age 62 or to a victim of identity theft who has submitted a copy of a valid investigative or incident report or complaint with a law enforcement agency about the unlawful use of the victim's identifying information by another person, or to the victim's spouse, and otherwise may charge a fee not to exceed \$3. *See* N.C. Gen. Stat. Ann. § 75-63(o).

These related consumer protection provisions—which a business may wish to note in a breach notification to consumers even in states where not required to do so—are discussed in section 27.08[12], 27.04[6][D] and catalogued in chapter 46 (identity theft).

Since September 2018, there is no charge in any state for placing a credit freeze on a consumer's account and obtaining yearlong fraud alerts.

language.<sup>2</sup> California, since January 1, 2016, also requires that a specific format be used for notice to consumers.<sup>3</sup>

**Hawaii**,<sup>4</sup> **Michigan**,<sup>5</sup> **North Carolina**<sup>6</sup> and **Vermont**<sup>7</sup> require that the notice be “clear and conspicuous” and include a description of the following details (which, without the “clear and conspicuous” language, are also required in notices sent to **Virginia**<sup>8</sup> residents):

- the incident in general terms (and, in Vermont, the “approximate date of the security breach”);
- the type of personal information (or “personally identifiable information” in Vermont) that was subject to the unauthorized “access and acquisition” (“access or use” in Michigan; “security breach” in Vermont<sup>9</sup>);
- the general acts of the business (or, if applicable,

<sup>2</sup>See Cal. Civ. Code §§ 1798.82(d)(1), 1798.29(d)(1); Wash. Rev. Code Ann. §§ 19.255.010(14), 42.56.590(13).

<sup>3</sup>Notices to California consumers must conform to a form notification breach letter approved by the California legislature in 2015, which must include sections titled: *What Happened*; *What Information was Involved*; *What We Are Doing*; *What You Can Do*; and *For More Information*. A copy of this form is reprinted in the California Code and may be found in section 27.09[6].

<sup>4</sup>Haw. Rev. Stat. Ann. § 487N-2(d).

<sup>5</sup>Mich. Comp. Laws Ann. § 445.72(6).

<sup>6</sup>N.C. Gen. Stat. § 75-65(d).

<sup>7</sup>Vt. Stat. Ann. tit. 9, § 2435(4).

<sup>8</sup>Va. Code Ann. § 18.2-186.6(A). Virginia’s statute applies only to individuals and entities, not government agencies. Even though the Virginia statute does not expressly require that the notice include “clear and conspicuous” it goes without saying that all notices sent to consumers pursuant to state security breach notification statutes should be drafted to be clear and conspicuous.

<sup>9</sup>A *security breach* is defined under Vermont law to mean

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.

Vt. Stat. Ann. tit. 9, § 2430(12)(A). The statute excludes from the definition of *security breach*

good faith but unauthorized acquisition of personally identifiable information by an employee or agent of the data collector for a legitimate purpose of the data collector, provided that the personally identifiable information is not used for a purpose unrelated to the data collector’s business or subject to further unauthorized disclosure.

*Id.* § 2430(12)(B). In determining whether personally identifiable information has been acquired or is reasonably believed to have been acquired by

government agency) undertaken to protect the personal information from further unauthorized access (or “the general acts of the data collector to protect the personally identifiable information from further security breach” in Vermont);

- a telephone number<sup>10</sup> (for the business, in North Caro-

a person without valid authorization, Vermont’s security breach statute provides that a data collector may consider the following factors, among others:

- (i) indications that the information is in the physical possession and control of a person without valid authorization, such as a lost or stolen computer or other device containing information;
- (ii) indications that the information has been downloaded or copied;
- (iii) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported; or
- (iv) that the information has been made public.

*Id.* § 2430(12)(C).

Vermont amended its security breach notification law effective January 1, 2019, to expressly require annual disclosures of security breaches by data brokers. *See generally supra* § 27.04[6][J]. A *data broker security breach* means “an unauthorized acquisition or a reasonable belief of an unauthorized acquisition of more than one element of brokered personal information maintained by a data broker when the brokered personal information is not encrypted, redacted, or protected by another method that renders the information unreadable or unusable by an unauthorized person.” Vt. Stat. Ann. tit. 9, § 2430(5)(A). The definition excludes, however, “good faith but unauthorized acquisition of brokered personal information by an employee or agent of the data broker for a legitimate purpose of the data broker, provided that the brokered personal information is not used for a purpose unrelated to the data broker’s business or subject to further unauthorized disclosure.” *Id.* § 2430(5)(B). In determining whether brokered personal information has been acquired or is reasonably believed to have been acquired by a person without valid authorization, “a data broker may consider the following factors, among others: (i) indications that the brokered personal information is in the physical possession and control of a person without valid authorization, such as a lost or stolen computer or other device containing brokered personal information; (ii) indications that the brokered personal information has been downloaded or copied; (iii) indications that the brokered personal information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported; or (iv) that the brokered personal information has been made public.” *Id.* § 2430(5)(C).

Data brokers also may be required to report data breaches shortly after they occur to the extent a data broker is also a *data collector* under Vermont state law.

<sup>10</sup>Vermont requires that the telephone number listed be a toll-free number, if available. Vt. Stat. Ann. tit. 9, § 2435(b)(5)(D).

- lina) that a person may call for further information and assistance, if one exists; and
- advice that directs recipients to remain vigilant by reviewing account statements and monitoring free credit reports (or in Michigan, a reminder of “the need to remain vigilant for incidents of fraud and identity theft”).

**North Carolina** additionally requires that notice to state residents include the toll-free numbers and addresses for major consumer reporting agencies and the toll-free numbers, addresses, and website address 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.

**Illinois** does not require disclosure of the cause of the breach but does require, at a minimum, disclosure of the toll free numbers and addresses for consumer reporting agencies, the toll free number, address and website address for the FTC and “a statement that the individual can obtain information from these sources about fraud alerts and security freezes.”<sup>11</sup>

**Iowa** further requires that a notice include, “at a minimum,” all of the following:

- the approximate date of the breach of security,
- contact information for consumer reporting agencies, and
- advice to the consumer to report suspected incidents of identity theft to local law enforcement or the attorney general.<sup>12</sup>

**Oregon** includes a list composed of most of these elements, in addition to contact information of the person that provides the notice.<sup>13</sup>

**New Hampshire** merely requires (1) a description of the incident in general terms, (2) the approximate date of the breach, (3) the type of personal information obtained as a result of the security breach, and (4) the telephonic contact

---

<sup>11</sup>815 Ill. Comp. Stat. Ann. 530/10(a), 530/12(a).

<sup>12</sup>Iowa Code Ann. § 715C.2(5). That statute also requires that the notice provide a description of the breach and the type of personal information obtained as a result of the breach, which are details required in the other states listed above and therefore were not repeated in the text.

<sup>13</sup>See Or. St. § 646A.604(5)(d).

information of the person subject to the security breach notification law.<sup>14</sup> **Missouri** requires the first and third categories listed above, in addition to a telephone number “that the affected consumer may call for further information and assistance, if one exists,” contact information for consumer reporting agencies and “[a]dvice that directs the affected consumer to remain vigilant by reviewing account statements and monitoring free credit reports.”<sup>15</sup>

**Florida** requires that notice include “at a minimum” (1) the “date, estimated date, or estimated date range” of the security breach, (2) a description of the personal information that was accessed or reasonably believed to have been accessed, and (3) “[i]nformation 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.”<sup>16</sup> **Alabama**, whose statute is modeled on Florida’s, includes the same three details as Florida (albeit phrased somewhat differently to account for the use of different terminology in the Alabama law) but also adds (4) a general description of the actions taken by a covered entity to restore the security and confidentiality of the personal information involved in the breach, and (5) a general description of the steps an affected individual can take to protect himself or herself from identity theft.<sup>17</sup>

**New York** law requires that, regardless of the method by which it is provided, the notice must 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 were, or are reasonably believed to have been, so acquired.”<sup>18</sup>

**Maryland**, like other states, requires a description of the categories of information that were or are reasonably believed to have been acquired,<sup>19</sup> the toll-free telephone numbers and addresses for the major consumer reporting

---

<sup>14</sup>31 N.H. Rev. Stat. Ann. § 359-C:20(IV).

<sup>15</sup>Mo. Rev. Stat. § 407.1500.2(4).

<sup>16</sup>Fla. Stat. Ann. § 501.171(4)(e).

<sup>17</sup>Ala. Code § 8-38-5(d).

<sup>18</sup>N.Y. Gen. Bus. L. § 899-aa(7).

<sup>19</sup>Md. Code Ann., Com. Law § 14-3504(g)(1) requires inclusion “[t]o

agencies,<sup>20</sup> and the contact information for the business making the notification (including the address, telephone number, and toll free telephone number “if one is maintained”).<sup>21</sup> However, Maryland also requires that consumer notice letters include the toll-free telephone numbers, addresses, and website addresses for the Federal Trade Commission and the Office of the Attorney General of Maryland and a statement that an individual can obtain information from these sources about steps that he or she can take to avoid identity theft.<sup>22</sup>

**Massachusetts** requires that a person or agency that owns or licenses data that includes personal information about a Massachusetts resident must advise consumers<sup>23</sup> of their “right to obtain a police report, how a consumer requests a security freeze and the necessary information to be provided when requesting a security freeze, and any fees required to be paid to any of the consumer reporting agencies.”<sup>24</sup> As of July 2008, the cost for Massachusetts residents to obtain a security freeze was \$5, although it may

---

the extent possible, [of] a description of the categories of information that were, or are reasonably believed to have been acquired by an unauthorized person, including which elements of personal information were, or are reasonably believed to have been, acquired . . . .” *Id.*

<sup>20</sup>Although *major consumer reporting agencies* is not expressly defined in the statute, the Maryland Attorney General’s website clarifies that notice must be sent to Equifax, Experian and TransUnion. See <http://www.oag.state.md.us/idtheft/businessGL.htm>. The contact information for reporting data breaches to those agencies is as follows:

|                                                      |                                                        |                                                            |
|------------------------------------------------------|--------------------------------------------------------|------------------------------------------------------------|
| Equifax                                              | Experian                                               | Transunion                                                 |
| Consumer Fraud Division                              | P.O. Box 2104                                          | P.O. Box 6790                                              |
| P.O. Box 740256                                      | Allen, TX 75013                                        | Fullerton, CA 92634-6790                                   |
| Atlanta, GA 30374                                    | DataBreachInfo                                         | 1-800-971-4307                                             |
| 1-888-766-0008                                       | @Experian.com                                          | <a href="http://www.transunion.com">www.transunion.com</a> |
| <a href="http://www.equifax.com">www.equifax.com</a> | 1-866-751-1323                                         |                                                            |
|                                                      | <a href="http://www.experian.com">www.experian.com</a> |                                                            |

<sup>21</sup>Md. Code Ann., Com. Law § 14-3504(g). The statute does not require a business to obtain a toll-free number; merely to list the number if it already has one.

<sup>22</sup>Md. Code Ann., Com. Law § 14-3504(g)(4).

<sup>23</sup>The disclosures required by section 3(b) of persons or agencies that own or license data must also be made to the Attorney and the director of consumer affairs and business relations.

<sup>24</sup>Mass. Gen. L. Ann. ch. 93H, § 3(b). In addition, a person or government agency that maintains or stores but does not own or license the data must inform the owner or licensor of the breach of security or unautho-

be higher today.

Massachusetts law also provides that a notice to consumers not “include the nature of the breach or unauthorized acquisition or use or the number” of affected Massachusetts residents.<sup>25</sup> As noted above, this is directly contrary to the laws of a number of states. For this reason, it will usually be necessary to use more than one version of the notice sent to consumers when an incident involves residents of Massachusetts and multiple other states.

**Rhode Island** requires that notice to consumers include, 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) Date of breach, estimated date of breach or the date range within which the breach occurred;
- (4) 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: (i) The credit reporting agencies; (ii) Remediation service providers; (iii) 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 requests 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 agencies.<sup>26</sup>

**West Virginia** requires that the notice 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 an individual may use to contact the

---

rized acquisition or use, the date or approximate date of the incident, the nature of the incident and any steps taken or planned to be taken relating to the incident. Mass. Gen. L. Ann. ch. 93H, § 3(a).

<sup>25</sup>Mass. Gen. L. Ann. ch. 93H, § 3(a).

<sup>26</sup>R.I. Gen. Laws § 11-49.3-4(d).

entity (or an agent of the entity) to learn: (a) what type of information the entity maintained about the 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.<sup>27</sup>

**Wisconsin** requires that where a business with a principal place of business located outside Wisconsin that “knows that personal information pertaining to a resident of this state has been acquired by a person whom the entity has not authorized to acquire the personal information,” then the entity must in its notice “indicate that the entity knows of the unauthorized acquisition of personal information pertaining to” the subject of the personal information.<sup>28</sup> Upon written request by a recipient of a notice of breach—but inferentially *not* in the actual notice itself—the entity must also “identify the personal information that was acquired.”<sup>29</sup>

Because of these varied requirements, persons or entities required to provide notice to consumers may elect to send separate letters to residents of certain states, rather than a single letter to residents of all jurisdictions. For example, a separate letter may be sent to **Massachusetts** residents because of the legal requirement that the nature of the breach not be disclosed to state residents, which is the opposite of what is required under a number of other states’ security breach notification laws. Likewise, a separate letter could be prepared for Maryland residents based on the **Maryland** requirement that the contact information for the Office of Maryland’s Attorney General be provided<sup>30</sup> (unless the sender intends to also include the contact information for the Attorneys General of all affected states or be willing to field questions from recipients in other jurisdictions about why information for their states was omitted).<sup>31</sup>

For breaches by government entities or their contractors, **Minnesota** provides that written notice must be given to consumers informing them that a report will be prepared,

---

<sup>27</sup>W. Va. Code § 46A-2A-102(d).

<sup>28</sup>Wis. Stat. Ann. § 134.98(2).

<sup>29</sup>Wis. Stat. Ann. § 134.98(3)(c).

<sup>30</sup>Md. Code Ann., Com. Law § 14-3504(g)(4)(i)(2).

<sup>31</sup>*See supra* § 27.08[1].

how they may obtain a copy and that the individual may request delivery by mail or email.<sup>32</sup> The report, in turn, must include:

- (1) a description of the type of data that were accessed or acquired;
- (2) the number of individuals whose data was improperly accessed or acquired;
- (3) if there has been final disposition of disciplinary action, the name of each employee determined to be responsible for the unauthorized access or acquisition, unless the employee was performing certain official duties; and
- (4) the final disposition of any disciplinary action taken against each employee in response.<sup>33</sup>

**California** amended its security breach notification statutes effective 2012 to require that notices be “written in plain language”<sup>34</sup> and incorporate specific mandatory and optional disclosures (drawn largely from some of the other state requirements discussed above) including, for businesses and individuals, “at a minimum” the following information:

- The name and contact information of the reporting person or business subject to this section.
- A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
- If the information is possible to determine at the time the notice is provided, then any of the following:
  - the date of the breach,
  - the estimated date of the breach,
  - the date range within which the breach occurred.
  - the date of the notice.
- Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.
- A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
- The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a

---

<sup>32</sup>Minn. Stat. Ann. § 13.055(2)(a).

<sup>33</sup>See Minn. Stat. Ann. § 13.055(2)(b).

<sup>34</sup>Cal. Civ. Code §§ 1798.82(d)(1), 1798.29(d)(1).

Social Security number or a driver's license or California identification card number.<sup>35</sup>

The statute also provides that the notice *may* include any of the following information, at the discretion of the person or business:

- Information about what the agency has done to protect individuals whose information has been breached.
- Advice on steps that the person whose information has been breached may take to protect himself or herself.<sup>36</sup>

California also includes an odd requirement with respect to the notice that must be provided *if* the person or business that was the source of the breach elects to provide identity theft prevention and mitigation services. California law does not actually require that identity theft prevention or mitigation services, such as credit monitoring, be provided. California's security breach notification law provides, however, that *if* identity theft prevention and mitigation services are offered, and if the person or business providing notification was the source of the breach, then the offer to provide identity theft prevention and mitigation services must be included in the notice to any person whose information was or may have been breached if the breach exposed personal information (as defined under the California security breach notification law) and the notice must state that it will be provided at no cost to the affected person for not less than 12 months, and provide the information necessary to take advantage of the offer.<sup>37</sup> This odd formulation—requiring specific disclosures and a time period *if* identity theft prevention and mitigation services are offered, without the express requirement that these services be offered—represented a legislative compromise at the time California's security breach notification law was amended.

**Oregon**, like California, adopted disclosure rules in 2018 in the event credit monitoring or identity theft and prevention services are offered following a breach, but does not require that these services be offered. If a person must notify a consumer of a breach of security and, in connection with

---

<sup>35</sup>Cal. Civ. Code § 1798.82(d)(2); *see also* Cal. Civ. Code § 1798.29(d)(2) (imposing parallel obligations on state agencies).

<sup>36</sup>Cal. Civ. Code § 1798.82(d)(3); *see also* Cal. Civ. Code § 1798.29(d)(3) (imposing parallel obligations on state agencies).

<sup>37</sup>Cal. Civ. Code § 1798.82(d)(2)(H).

the notification, offers to provide credit monitoring services or identity theft prevention and mitigation services without charge to the consumer, then Oregon law provides that the person may not condition the person's provision of the services on the consumer's providing the person with a credit or debit card number or on the consumer's acceptance of any other service the person offers to provide for a fee.<sup>38</sup> Conversely, if a person offers additional credit monitoring services or identity theft prevention and mitigation services for a fee, the person must "separately, distinctly, clearly and conspicuously disclose in the offer for the additional credit monitoring services or identity theft prevention and mitigation services that the person will charge the consumer a fee."<sup>39</sup> Oregon law further provides that the terms and conditions of any contract under which one person offers or provides credit monitoring services or identity theft prevention and mitigation services on behalf of another person, in connection with notification of a security breach, must require compliance with the requirements set forth in this paragraph.<sup>40</sup>

By contrast, Connecticut and Delaware affirmatively mandate provision of these type of services.

**Connecticut** affirmatively requires that identity theft prevention and, if applicable, mitigation services, be provided to residents whose personal information was breached (or is reasonably believed to have been breached), free of charge, for not less than 24 months, and requires that notice of the availability of these services and information on placing a credit freeze on a consumer's credit file be provided, but not necessarily in the notice of breach.<sup>41</sup> Connecticut law requires that "all information necessary" for affected residents to enroll in identity theft prevention and, if applicable, mitigation services, along with information on how a resident can put a credit freeze on his or her credit file, be provided to affected residents.<sup>42</sup> As a practical matter, companies may find it more economical to include this information in the notice of breach to state residents—especially given that notice to the Connecticut Attorney General is required when security

---

<sup>38</sup>Or. Rev. Stat. Ann. § 646A.604(7)(a).

<sup>39</sup>Or. Rev. Stat. Ann. § 646A.604(7)(b).

<sup>40</sup>Or. Rev. Stat. Ann. § 646A.604(7)(c).

<sup>41</sup>See Conn. Gen. Stat. Ann. § 36a-701b(b)(2)(B).

<sup>42</sup>See Conn. Gen. Stat. Ann. § 36a-701b(b)(2)(B).

breach notification is provided to Connecticut residents.<sup>43</sup> On the other hand, if for some reason a company prefers to supply this information separately (for example, if appropriate services have not yet been secured by the time notice must be sent, or if there is concern about including this information in a letter to residents of one state but not others), Connecticut law appears to allow this.

**Delaware** followed Connecticut's lead in providing that, effective on or after April 14, 2018, if the security of personal information, including a social security number of a state resident, was breached or was "reasonably believed to have been breached, . . ." the resident must be provided with credit monitoring services at no cost to the resident for a period of one (1) year<sup>44</sup> (as well as all information necessary to enroll in a credit monitoring service and details on how to place a credit freeze on the resident's credit file).<sup>45</sup> These services are not required, however, "if, after an appropriate investigation, the person reasonably determines that breach of security is unlikely to result in harm to the individuals whose personal information has been breached."<sup>46</sup>

Credit monitoring and similar mitigations services are separately addressed in section 27.08[9].

Covered entities under HIPAA are exempt from complying with the specific requirements for the contents of a notice to California residents under California's breach notification statute for persons or businesses if it has complied completely with section 13402(f) of the federal Health Information Technology for Economic and Clinical Health Act, although it will not be exempt from any other provision of the California breach notification statute.<sup>47</sup>

**Washington** adopted in part the new California language in 2015. Under Washington law, notice must be written in plain language and include, at a minimum,

---

<sup>43</sup>See Conn. Gen. Stat. Ann. § 36a-701b(b)(2)(A); *see generally infra* § 27.08[8] (analyzing notification obligations to state agencies, including state attorneys general).

<sup>44</sup>Del. Code Ann. tit. 6, § 12B-102(e).

<sup>45</sup>Del. Code Ann. tit. 6, § 12B-102(e).

<sup>46</sup>Del. Code Ann. tit. 6, § 12B-102(e).

<sup>47</sup>See Cal. Civ. Code § 1798.82(e). There is no parallel provision for state agencies, which presumably are not also covered entities under HIPAA.

- The name and contact information of the reporting person or business subject to this section;
- A list of the types of personal information that were or are reasonably believed to have been the subject of a breach; and
- The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed personal information.<sup>48</sup>

**Wyoming** likewise amended its security breach notification law in 2015 to require “clear and conspicuous notice that includes, at a minimum:

- A toll-free number:
  - That the individual may use to contact the person collecting the data, or his agent; and
  - ◻ From which the individual may learn the toll-free contact telephone numbers and addresses for the major credit reporting agencies.
- The types of personal identifying information that were or are reasonably believed to have been the subject of the breach;
- A general description of the breach incident;
- The approximate date of the breach of security, if that information is reasonably possible to determine at the time notice is provided;
- In general terms, the actions taken by the individual or commercial entity to protect the system containing the personal identifying information from further breaches;
- Advice that directs the person to remain vigilant by reviewing account statements and monitoring credit reports;
- Whether notification was delayed as a result of a law enforcement investigation, if that information is reasonably possible to determine at the time the notice is provided.<sup>49</sup>

**New Mexico**, in its statute enacted in 2017, follows a similar approach in requiring that the following information be included in notices to consumers:

- the name and contact information of the notifying person;

---

<sup>48</sup>Wash. Rev. Code Ann. §§ 19.255.010(14), 42.56.590(13).

<sup>49</sup>Wyo. Stat. Ann. § 40-12-502(e)(vii).

- a list of the types of personal identifying information that are reasonably believed to have been the subject of a security breach, if known;
- the date of the security breach, the estimated date of the breach or the range of dates within which the security breach occurred, if known;
- a general description of the security breach incident;
- the toll-free telephone numbers and addresses of the major consumer reporting agencies;
- advice that directs the recipient to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach; and
- advice that informs the recipient of the notification of the recipient's rights pursuant to the federal Fair Credit Reporting Act.<sup>50</sup>

Statutes modeled on California's original 2003 notification breach statutes do not include these specific content requirements, which were drawn from subsequent modifications by other states to California's original law, as noted above.

### **27.08[7] Additional Notices to Credit Reporting Agencies**

In addition to notice to consumers, a number of states require that notice be provided to consumer reporting agencies under certain circumstances. The requirement to provide notice to credit reporting agencies is phrased somewhat differently under different statutes. Accordingly, some states appear to require that prior notice be provided to credit reporting agencies,<sup>1</sup> while others provide for subsequent notice<sup>2</sup> or are indifferent to the order in which consumer and

---

<sup>50</sup>N.M. Stat. Ann. § 57-12C-7.

#### **[Section 27.08[7]]**

<sup>1</sup>For example, Colorado requires notice to all consumer credit reporting agencies that compile and maintain files on consumers on a nationwide basis (as defined in the Fair Credit Reporting Act) "in the most expedient time possible and without unreasonable delay" if a covered entity is required to provide a breach notice to more than one thousand Colorado residents, disclosing "the anticipated date of the notification to the residents and the approximate number of residents who are to be notified . . . ." Colo. Rev. Stat. Ann. § 6-1-716(2)(d) (emphasis added).

<sup>2</sup>For example, Michigan provides that notice to consumer reporting agencies be sent "after a person or agency provides a notice . . ." to consumers about the breach. Mich. Comp. Laws Ann. § 445.72(8)

credit reporting agency notices are sent.<sup>3</sup>

Most statutes require notice to credit bureaus for breaches over a certain size. **South Dakota's** law, however, requires notice to credit reporting agencies any time notification to consumers is required, laying out "the timing, distribution, and content of the notice."<sup>4</sup>

Under **Rhode Island** law, notice to major credit reporting agencies of the timing, content and distribution of the notices and the approximate numbers of affected individuals if more than 500 Rhode Island residents will receive notice.<sup>5</sup>

Some states, such as **Alabama**,<sup>6</sup> **Alaska**,<sup>7</sup> **Colorado**, **Florida**,<sup>8</sup> **Hawaii**, **Indiana**, **Kansas**, **Kentucky**,<sup>9</sup> **Michigan** (for persons or agencies not otherwise subject to title V of the Gramm-Leach-Bliley Act), **Minnesota** (in the case of

---

(emphasis added). By contrast, Wisconsin, less directly, merely requires that if, as a result of a single incident, an entity is required to provide notice to 1,000 or more individuals, it must notify consumer reporting agencies "without unreasonable delay" of "the timing, distribution, and content of the notices sent to individuals." Wis. Stat. Ann. § 134.98(2)(br).

<sup>3</sup>For example, Maine requires that notification include "the actual or anticipated date that persons were or will be notified of the breach." Me. Rev. Stat. Ann. tit. 10, § 1348(4).

<sup>4</sup>S.D. Codified Laws § 22-40-24 ("If an information holder discovers circumstances that require notification pursuant to § 22-40-20 the information holder shall also notify, without unreasonable delay, all consumer reporting agencies, as defined under 15 U.S.C. § 1681a in effect as of January 1, 2018, and any other credit bureau or agency that compiles and maintains files on consumers on a nationwide basis, of the timing, distribution, and content of the notice.").

<sup>5</sup>R.I. Gen. Laws § 11-49.3-4(a)(2). This notice must be made without delaying notice to Rhode Island consumers. *Id.*

<sup>6</sup>Ala. Code § 8-38-7.

<sup>7</sup>Alaska requires that this notice, like notice to consumers, "also notify without unreasonable delay" consumer reporting agencies, but makes clear that this requirement may not be construed to require disclosure of the names or other personal information of the state residents whose personal information was subject to the breach. Alaska Stat. § 45.48.040.

<sup>8</sup>Fla. Stat. Ann. § 501.171(5).

<sup>9</sup>Ky. Rev. Stat. Ann. § 365.732(7). Kentucky's statute provides that if consumer notice must be provided to more than 1,000 people at one time, notice must also be provided, "without unreasonable delay, [to] 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." Ky. Rev. Stat. Ann. § 365.732(7).

state agencies), **Nevada**, **New Hampshire** (for persons or agencies not otherwise subject to title V of the Gramm-Leach-Bliley Act), **New Jersey**, **North Carolina**, **Ohio**, **Oregon**,<sup>10</sup> **Pennsylvania**, **South Carolina**, **Tennessee**, **Vermont** (subject to an exception for persons licensed by the department of financial regulation) and **Wisconsin**, require notice to credit reporting agencies when more than 1,000 consumers will receive notice.

**Georgia** and **Maine** have a similar provision in force, applicable if an information broker (or a person under Maine law) is required to notify more than 10,000 consumers in the case of Georgia, or 1,000 in the case of Maine. **Texas**<sup>11</sup> likewise requires notice to consumer reporting agencies if notification will be provided to more than 10,000 persons at one time. The Maine statute specifically requires notice of the number of persons affected by the breach, if known, and the actual or anticipated date that persons were or will be given notice.<sup>12</sup>

**New York** similarly requires that notice to credit reporting agencies be provided about the timing, contents and distribution of consumer notices (and the approximate number of affected persons) if more than 5,000 New York residents will be notified at one time, without delaying notice to affected New York residents.

**Florida**,<sup>13</sup> **Maryland**<sup>14</sup> and **West Virginia** require notice to consumer reporting agencies “without unreasonable delay” “of the timing, distribution and content” of the notices (but not the names or other personally identifying information of breach notice recipients) if an entity is required to notify more than 1,000 persons of a breach and in West Virginia is not otherwise subject to Title V of the Gramm Leach Bliley Act. **Minnesota** requires individuals and businesses to provide notice to credit reporting agencies within forty-eight hours of discovering circumstances requiring notification to more than 500 persons at one time.

If applicable, **Michigan** requires that notice be sent to

---

<sup>10</sup>Or. Rev. Stat. Ann. § 646A.604(6).

<sup>11</sup>Tex. Bus. & Comm. Code § 521.053(h); *see also* Tex. Gov’t Code §§ 205.010, 2054.1125 (applying the provision to state and local governments).

<sup>12</sup>Me. Rev. Stat. Ann. tit. 10, § 1348(4).

<sup>13</sup>Fla. Stat. Ann. § 501.171(5).

<sup>14</sup>Md. Code Ann., Com. Law § 14-3506.

each consumer reporting agency *after* consumer notices have been sent out. Michigan law stipulates that the notice must include the number of notices provided to residents of Michigan and the timing of those notices.<sup>15</sup>

**Missouri** requires that where notice to more than 1,000 consumers at one time will be provided, notice must also be given “without unreasonable delay . . .” to “all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis . . . of the timing, distribution and contents of the notice.”<sup>16</sup>

**Montana** law provides that if a business “suggests, indicates, or implies” in a security breach notice that an individual may obtain a copy of its credit report, it must “coordinate with the consumer reporting agency as to the timing, content, and distribution” of the notice, but may not “unreasonably delay the notice to the affected individuals.”<sup>17</sup>

**Oregon** requires that the police report number for the security breach, if available, must be included in the notice to credit reporting agencies.<sup>18</sup> The obligation to notify consumer reporting agencies, however, may not delay the provision of notice to consumers otherwise required by the statute.<sup>19</sup>

Statutes typically require notice of the date when notice to consumers will be sent and the approximate number of state residents affected.<sup>20</sup> **South Carolina**, however, also mandates disclosure of the timing, distribution and content of notice to consumers.<sup>21</sup> No statute requires disclosure of the names of affected residents and indeed some expressly provide that personally identifying information should not be included in any notice to credit bureaus.

### 27.08[8] Additional or Alternative Notices to State Agencies

Many but not all states require that notice be provided to state agencies or officials prior to, at the same time as, or right after notice of a breach is provided to consumers. Some

---

<sup>15</sup>Mich. Comp. Laws Ann. § 445.72(8).

<sup>16</sup>Mo. Rev. Stat. § 407.1500.2(8).

<sup>17</sup>Mont. Code Ann. § 30-14-1704(7).

<sup>18</sup>Or. Rev. Stat. Ann. § 646A.604(6).

<sup>19</sup>Or. Rev. Stat. Ann. § 646A.604(6).

<sup>20</sup>*See, e.g.*, Colo. Rev. Stat. Ann. § 6-1-716(2)(d).

<sup>21</sup>S.C. Code Ann. §§ 1-11-490(I) (agencies), 39-1-90(K) (persons).

state laws stipulate what should be in the notice to a state agency and when it must be sent. Four states —**Alaska**,<sup>1</sup> **Florida**,<sup>2</sup> **South Dakota**,<sup>3</sup> and **Vermont**<sup>4</sup>— also require notice to the state under certain circumstances when it is determined that notice to consumers need not be provided (and other states require retention of written documentation of this determination, which regulators in those states potentially could request in the event of an investigation).

Some jurisdictions, including **California**,<sup>5</sup> **Connecticut**,<sup>6</sup> **Delaware**,<sup>7</sup> **Florida**,<sup>8</sup> **Hawaii**,<sup>9</sup> **Illinois**,<sup>10</sup> **Indiana**,<sup>11</sup> **Iowa**,<sup>12</sup> **Louisiana** (by administrative regulation),<sup>13</sup> **Maine**,<sup>14</sup> **Maryland**,<sup>15</sup> **Massachusetts**,<sup>16</sup> **Missouri**,<sup>17</sup> **Montana**,<sup>18</sup> **Ne-**

---

[Section 27.08[8]]

<sup>1</sup>Alaska Stat. § 45.48.010(c).

<sup>2</sup>Fla. Stat. Ann. § 501.171(4)(c).

<sup>3</sup>S.D. Codified Laws § 22-40-20.

<sup>4</sup>Vt. Stat. Ann. tit. 9, § 2435(d)(1). The notice may be designated as a trade secret and treated confidentially if applicable. *See id.* If a data collector subsequently determines that misuse in fact has occurred or is occurring, however, it must provide notice to consumers as otherwise required by Vermont law. *Id.* § 2435(d)(2).

<sup>5</sup>*See* Cal. Civ. Code §§ 1798.29(e), 1798.82(f).

<sup>6</sup>*See* Conn. Gen. Stat. Ann. §§ 36a-701b(b)(2), 36a-701b(f).

<sup>7</sup>Del. Code Ann. tit. 6, § 12B-102(d).

<sup>8</sup>*See* Fla. Stat. Ann. § 501.171(3) (requiring notice to the Department of Legal Affairs of any breach affecting 500 or more Florida residents, within thirty days after determination of the breach or reason to believe a breach occurred).

<sup>9</sup>*See* Haw. Rev. Stat. Ann. § 487N-2(f) (requiring notice to Hawaii's Office of Consumer Protection whenever notice is sent to more than 1,000 people at a time).

<sup>10</sup>815 Ill. Comp. Stat. Ann. 530/12(e) (applicable to state agencies). Illinois requires a state agency generally to provide notice to the Attorney General within 45 days of discovery of the breach or when notice is provided to consumers, whichever is sooner, except where there is good cause for reasonable delay.

<sup>11</sup>*See* Ind. Code § 24-4.9-3-1(c).

<sup>12</sup>Iowa Code Ann. § 715C.2(8).

<sup>13</sup>*See* Reporting Requirements, La. Admin. Code tit. 16, III § 701 (Mar. 2007).

<sup>14</sup>*See* Me. Rev. Stat. Ann. tit. 10, § 1348(5).

<sup>15</sup>Md. Code Ann., Com. Law § 14-3504(h). Although the statute compels prior notice to the Attorney General (and does not identify any

**braska,<sup>19</sup> New Hampshire,<sup>20</sup> New Mexico,<sup>21</sup> New York,<sup>22</sup> North Carolina,<sup>23</sup> North Dakota,<sup>24</sup> Oregon,<sup>25</sup> Rhode Island,<sup>26</sup> South Carolina,<sup>27</sup> South Dakota,<sup>28</sup> Puerto Rico,<sup>29</sup>**

particular information that must be included in this notice), the Attorney General's Office will seek further information if a copy of the notice sent to consumers is not included in the notice to the Attorney General's Office. As a practical matter, the Attorney General's notice probably should include a draft of the final letter in view of the required timing for providing notice to the Attorney General prior to giving notice to consumers.

<sup>16</sup>Notice of the same details required to be included in notices sent to consumers by an agency or person that owns or licenses data that includes personal information must be also be provided by the agency or person to the Massachusetts Attorney General and the director of consumer affairs and business relations. *See* Mass. Gen. L. Ann. ch. 93H, § 3(b). Upon receipt of the notice, the director of consumer affairs and business relations will identify "any relevant consumer reporting agency or state agency" and forward their names to the agency or person, who will then be required to provide notice to them "as soon as practicable and without unreasonable delay . . . ." Mass. Gen. L. Ann. ch. 93H, § 3(b). Where consumer notice is not required because the person or agency has provided notice pursuant to federal laws, regulations, guidance, or guidelines (*supra* § 27.08[2]), the notice to be provided to the [A]ttorney [G]eneral and director of the office of consumer affairs and business regulations "shall consist of, but not be limited to, any steps the person or agency has taken or plans to take relating to the breach pursuant to the applicable federal law, rule, regulation, guidance or guidelines . . . ." Mass. Gen. L. Ann. ch. 93H, § 5.

<sup>17</sup>Mo. Rev. Stat. § 407.1500.2(8).

<sup>18</sup>Mont. Code Ann. § 30-14-1704(b)(8); Mont. Code Ann. § 2-6-1503(5) (as applicable to notice by state agencies).

<sup>19</sup>Neb. Rev. Stat. § 87-803(2).

<sup>20</sup>31 N.H. Rev. Stat. Ann. § 359-C:19(I)(b).

<sup>21</sup>N.M. Stat. Ann. § 57-12C-10.

<sup>22</sup>N.Y. Gen. Bus. L. § 899-aa(8)(a).

<sup>23</sup>*See* N.C. Gen. Stat. Ann. § 75-65(e1).

<sup>24</sup>*See* N.D. Cent. Code § 51-30-02.

<sup>25</sup>*See* Or. Rev. Stat. Ann. §§ 646A.604(1)(b) (notice to the Attorney General, if the number of consumers to receive notice exceeds 250), 646A.604(10) (requiring a copy of the notice to consumers be provided to the Attorney General).

<sup>26</sup>R.I. Gen. Laws § 11-49.3-4(a)(2).

<sup>27</sup>*See* S.C. Code Ann. §§ 1-11-490(I) (agencies), 39-1-90(K) (persons).

<sup>28</sup>S.D. Codified Laws § 22-40-20. Notice to the Attorney General is required when a breach impacts more than 250 state residents. *See id.*

<sup>29</sup>*See* 10 L.P.R. Ann. §§ 4052, 4051(b), 4054a.

**Vermont**<sup>30</sup> and **Washington**<sup>31</sup> require that notice be provided to particular state (or Commonwealth) consumer affairs agencies or the Attorney General before, at the same time as, or after notice is sent to consumers (and in some cases, even when notice to consumers is not required). For example, **Maine** requires notice to “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.”<sup>32</sup> **New Mexico** requires that notice be provided to the Attorney General and major consumer reporting agencies within forty-five (45) calendar days by a person required to issue a security breach notice to more than one thousand (1,000) New Mexico residents as a result of a single data breach.<sup>33</sup> **New York** law provides that if any New York residents are to be notified, notice about the timing, content and distribution of the notices and approximate number of affected persons must also be given to the state Attorney General, the consumer protection board and the state office of cybersecurity and critical infrastructure coordination.<sup>34</sup> **North Dakota** requires that notice be provided to the state attorney general by mail or email any time a breach affects more than two hundred and fifty people.<sup>35</sup> **Oregon** mandates written or electronic notice to the Attorney General whenever the number of consumers to whom a security breach notice is sent exceeds 250.<sup>36</sup> **Rhode Island** requires notice to the attorney general of the timing, content and distribution of the notices to consumers and the approximate numbers of affected individuals, if more than 500 Rhode Island residents will receive notice.<sup>37</sup> **South Carolina** includes a similar provision but notice must be sent to the Consumer Protection Division of South Carolina’s Department of Consumer Affairs (and to credit reporting

---

<sup>30</sup>See Vt. Stat. Ann. tit. 9, § 2435(b)(3).

<sup>31</sup>Wash. Rev. Code Ann. § 19.255.010(15); Wash. Rev. Code Ann. § 42.56.590(14).

<sup>32</sup>See Me. Rev. Stat. Ann. tit. 10, § 1348(5).

<sup>33</sup>See N.M. Stat. Ann. § 57-12C-10.

<sup>34</sup>N.Y. Gen. Bus. L. § 899-aa(8)(a).

<sup>35</sup>See N.D. Cent. Code § 51-30-02.

<sup>36</sup>See Or. Rev. Stat. Ann. § 646A.604(1)(b). The specific notice prescribed is set forth in section 604(1)(a).

<sup>37</sup>R.I. Gen. Laws § 11-49.3-4(a)(2). This notice must be made without delaying notice to Rhode Island consumers. *Id.*

agencies), but not to the Attorney General.<sup>38</sup> **Indiana** requires notice to the Attorney General and to the database owner's primary regulator, if the database owner is regulated.<sup>39</sup> Under **New Hampshire** law, notice must be provided to the regulator that has primary regulatory authority or, if none, the state's Attorney General.<sup>40</sup>

Pursuant to a 2011 amendment to its breach notification statutes, **California** requires that a single sample copy of the security breach notification sent to consumers—excluding any personally identifiable information—be submitted electronically to the California Attorney General, any time a person, business or government agency is required to issue such a notice to more than 500 California residents “as a result of a single breach of the security system . . . .”<sup>41</sup> **Washington** includes the same provision, but also requires that the notice to the Attorney General identify the number of Washington consumers affected by the breach (or an estimate if the exact number is not known).<sup>42</sup> Statutes modeled on California's original breach notification laws would not include this provision unless they have been modified or amended since the time they were first enacted.

**Connecticut**<sup>43</sup> and **Nebraska**<sup>44</sup> require that where notice to state residents is required, notice also be provided to the Attorney General “not later than the time when notice is provided” to a state resident.

**Delaware** requires notice to the Attorney General within the timeframe required for sending notice to consumers, if more than 500 state residents would be affected.<sup>45</sup>

**Florida** and **Alabama** stipulate the information that must be included in a notice to state officials and when it

---

<sup>38</sup>S.C. Code Ann. §§ 1-11-490(I) (agencies), 39-1-90(K) (persons).

<sup>39</sup>Ind. Code § 24-4.9-3-1(c).

<sup>40</sup>31 N.H. Rev. Stat. Ann. § 359-C:20(I)(b). The notice must include the anticipated date of sending out consumer notification letters and the “approximate number of individuals.” 31 N.H. Rev. Stat. Ann. § 359-C:20(I)(b).

<sup>41</sup>Cal. Civ. Code §§ 1798.29(e), 1798.82(f).

<sup>42</sup>See Wash. Rev. Code Ann. § 19.255.010(15); Wash. Rev. Code Ann. § 42.56.590(14).

<sup>43</sup>Conn. Gen. Stat. Ann. §§ 36a-701b(b)(2), 36a-701b(f).

<sup>44</sup>Neb. Rev. Stat. § 87-803(2).

<sup>45</sup>Del. Code Ann. tit. 6, § 12B-102(d).

must be provided. Florida requires that notice be provided to the Department of Legal Affairs within thirty days of the determination of a breach or reason to believe a breach occurred (and allows covered entities during that time period to petition the Department for an additional fifteen days to provide notice to consumers, which otherwise also generally must be given within thirty days, if good cause for the delay can be shown in writing to the department).<sup>46</sup> For a covered entity that is the judicial branch, the Executive Office of the Governor, the Department of Financial Services, or the Department of Agriculture and Consumer Services, in lieu of providing the written notice to the Department of Legal Affairs, the covered entity may post the required information on an agency-managed website.<sup>47</sup> Alabama requires that if the number of individuals that a covered entity is required to provide notice to exceeds 1,000, the entity must provide written notice of the breach to the Alabama Attorney General “as expeditiously as possible and without unreasonable delay” within 45 days of the covered entity’s determination, or receipt of notice from a third party agent, that a breach has occurred “and is reasonably likely to cause substantial harm to the individuals to whom the information relates.”<sup>48</sup> Both states require covered entities that are obligated to provide this type of notice, to provide a synopsis of the events that led to the breach, the approximate number of state residents affected, any services offered without charge (such as credit monitoring) and how to access it and contact information for an employee or agent (such as outside counsel) to whom further inquiries may be directed.<sup>49</sup> Florida also requires a copy of the actual notice sent to consumers or, if

---

<sup>46</sup>Fla. Stat. Ann. § 501.171(3)(a).

<sup>47</sup>Fla. Stat. Ann. § 501.171(3)(e).

<sup>48</sup>Ala. Code § 8-38-6(a). A covered entity is permitted to supplement or update information regarding the breach at any time, *Id.* § 8-38-6(c). A covered entity also may submit information marked confidential, which will not be “subject to any open records, freedom of information, or other public record disclosure law.” *Id.* § 8-38-6(d).

<sup>49</sup>*See* Ala. Code § 8-38-6(b); Fla. Stat. Ann. § 501.171(3)(a). Written notice to the Attorney General under Alabama letter must include –

- (1) A synopsis of the events surrounding the breach at the time that notice is provided.
- (2) The approximate number of individuals in the state who were affected by the breach.

none, a written explanation.<sup>50</sup>

**Iowa** requires any person who owns or licenses computerized data that includes a consumer's personal information that is used in the course of the person's business, vocation, occupation, or volunteer activities and that was subject to a breach of security requiring notification to more than 500 residents of Iowa pursuant to Iowa's security breach notification statute to give written notice of the breach following discovery or receipt of notification under Iowa Code Ann. § 715C.2(2) (from anyone who maintains or otherwise possesses personal information on behalf of the owner or licensor) to the director of the consumer protection division of the office of the attorney general within five business days after giving notice of the security breach to any consumer pursuant section 715C.2.<sup>51</sup>

By administrative regulation, **Louisiana** requires that when notice of a security breach is required under Louisiana

- 
- (3) Any services related to the breach being offered or scheduled to be offered, without charge, by the covered entity to individuals, and instructions on how to use the services.
  - (4) The name, address, telephone number, and email address of the employee or agent of the covered entity from whom additional information may be obtained about the breach.

Ala. Code § 8-38-6(b).

<sup>50</sup>Fla. Stat. Ann. § 501.171(3)(a). The notice, under Florida law, 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 (4) or an explanation of the other actions taken pursuant to subsection (4).
- 5. The name, address, telephone number, and e-mail address of the employee or agent of the covered entity from whom additional information may be obtained about the breach.

*Id.* § 501.171(3)(b). A covered entity also must provide the following information to the Department, upon request:

- 1. A police report, incident report, or computer forensics report.
- 2. A copy of the policies in place regarding breaches.
- 3. Steps that have been taken to rectify the breach.

*Id.* § 501.171(3)(c). A covered entity may provide supplemental information at any time. *Id.* § 501.171(3)(d).

<sup>51</sup>Iowa Code Ann. § 715C.2(8).

law, the person or agency providing notice must also provide written notice detailing the breach to the Consumer Protection section of the Attorney General's Office. The notice must include the names of all Louisiana citizens affected by the breach<sup>52</sup> and must be received within ten days of the distribution of consumer notices to Louisiana citizens. Failure to provide timely notice to the Attorney General may be punishable by a fine of up to \$5,000 per violation (with each day that notice is not received deemed a separate violation).<sup>53</sup> Notice must be mailed to:

Louisiana Department of Justice  
Office of the Attorney General  
Consumer Protection section  
1885 N. Third Street  
Baton Rouge, LA 70802<sup>54</sup>

**Missouri** requires that where notice to more than 1,000 consumers at one time will be provided, the Attorney General's Office also must be given notice "of the timing, distribution and contents of the notice" of the notice given to consumers "without unreasonable delay . . . ."<sup>55</sup>

When notice is provided to consumers, **North Carolina** requires that notice be provided "without unreasonable delay" to the Consumer Protection Division of the Attorney General's Office identifying the nature of the breach, the number of consumers affected by it, the steps taken to investigate the breach, the steps taken to prevent a similar breach in the future and information regarding the timing, distribution and contents of the notice.<sup>56</sup>

Although not apparent from the face of the statute, the

---

<sup>52</sup>Reporting Requirements, La. Admin. Code tit. 16, § 701(A) (2007).

<sup>53</sup>See Reporting Requirements, La. Admin. Code tit. 16, § 701(B) (2007).

<sup>54</sup>See Reporting Requirements, La. Admin. Code tit. 16, § 701(C) (2007).

<sup>55</sup>Mo. Rev. Stat. § 407.1500.2(8).

<sup>56</sup>N.C. Gen. Stat. Ann. § 75-65(e1). Where notice is provided to more than 1,000 people at one time, North Carolina further requires notice "without unreasonable delay" to the Consumer Protection Division of the Attorney General's Office *and* all credit reporting agencies that compile and maintain files on consumers on a nationwide basis, of the timing, distribution and content of the notice. N.C. Gen. Stat. Ann. § 75-65(f); *see*

North Carolina Department of Justice requires that companies not simply report the breach but also complete the North Carolina Security Breach Reporting Form, a copy of which is included in the Appendix to this chapter.<sup>57</sup> North Carolina also has a special statute dealing with data held by car dealerships, which requires that notice be provided in the event of a security breach.<sup>58</sup>

**Puerto Rico's** security breach notification statute requires that notice be given to the Department of Consumer Affairs within "a non-extendable term of ten (10) days after the violation" and directs the Department to make a public announcement of the breach within twenty-four hours after having received this information.<sup>59</sup>

**Vermont** requires that a preliminary description of the breach along with the date of the breach and date of discovery be provided to the Attorney General in many cases within fourteen days discovery of the breach or provision of notice to consumers, whichever is sooner.<sup>60</sup> When notice to consumers is sent, a copy of the notice must also be sent to the Attorneys General with information on the number of affected Vermont consumers, if known.<sup>61</sup> A data collector may send the Attorney General a second, redacted copy of the notice, omitting the type of personally identifiable information that was subject to the breach, to use for any public

---

*generally supra* § 27.08[7] (analyzing the requirement under some state statutes to provide notice to credit reporting agencies).

<sup>57</sup>The form was developed in an effort to standardize North Carolina's breach reporting process and the information obtained by the North Carolina Department of Justice. A copy of the form may also be obtained at [www.noscamnc.gov](http://www.noscamnc.gov).

<sup>58</sup>*See* N.C. Gen. Stat. Ann. § 20-305.7.

<sup>59</sup>10 L.P.R. Ann. §§ 4052, 4051(b).

<sup>60</sup>Vt. Stat. Ann. tit. 9, § 2435(b)(3)(A)(i). This obligation is tempered by the proviso that is subject to the legitimate needs of law enforcement. *See id.* In addition, notice to the Attorney General need only be provided prior to notice to consumers where a data collector, prior to a breach, had sworn in writing that it maintains "written policies and procedures to maintain the security of personally identifiable information and respond to a breach in a manner consistent with Vermont law . . . ." *Id.* § 2435(b)(3)(A)(ii). The form to make the certification to avoid the fourteen day notice requirement may be accessed from the website for the Vermont Attorney General's Office. *See* <http://www.atg.state.vt.us/assets/files/2012-06-29%2014-day%20Affirmation.pdf>

<sup>61</sup>Vt. Stat. Ann. tit. 9, § 2435(b)(3)(B)(i).

disclosure of the breach.<sup>62</sup>

Where notice under state law is not required because notice is or will be provided pursuant to federal laws, such as the Gramm-Leach-Bliley Act,<sup>63</sup> the Health Insurance Portability and Accountability Act (HIPAA)<sup>64</sup> or other federal or state laws,<sup>65</sup> or in accordance with a company's information security policy,<sup>66</sup> notice to the state Attorney General or other agency that consumer notice was sent to state residents pursuant to these other laws may be required for residents of a small number of states.<sup>67</sup> Most states, however, do not

---

<sup>62</sup>See Vt. Stat. Ann. tit. 9, § 2435(b)(3)(B)(ii); *see generally infra* § 27.09[49] (reprinting Vt. Stat. Ann. tit. 9, § 2435).

<sup>63</sup>See *supra* § 27.04[3].

<sup>64</sup>See *supra* § 27.04[4].

<sup>65</sup>See *supra* § 27.08[2] (enumerating exceptions based on notice requirements imposed by federal law or other state laws).

<sup>66</sup>See *supra* § 27.08[2].

<sup>67</sup>See, e.g., Conn. Gen. Stat. Ann. § 36a-701b(f); Fla. Stat. Ann. § 501.171(4)(g); Mass. Gen. Laws Ann. ch. 93H, § 5; Neb. Rev. Stat. § 87-804. For example, Florida requires timely provision to the Department of Legal Affairs of a copy of the notice sent pursuant to rules, regulations, procedures or guidelines established by a covered entity's primary or functional federal regulator. Fla. Stat. Ann. § 501.171(4)(g).

**Connecticut's** security breach statute provides that any person 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 Connecticut's notification statute, shall be deemed to be in compliance with the security breach notification law if it complies with its procedures and notifies the Attorney General not later than the time when notice is provided to the resident. Conn. Gen. Stat. Ann. § 36a-701b(f). Similarly, any person that provides notice pursuant to "the rules, regulations, procedures or guidelines established by the primary or functional regulator, as defined in 15 USC 6809(2)," will be deemed to be in compliance with the security breach notification statute if it provides notice as required by the regulator and notifies the Attorney General not later than the time when notice is provided to the resident. *Id.* **Nebraska** law is largely the same. See Neb. Rev. Stat. § 87-804 (notice pursuant to one's own information security policy or guidelines established by one's primary or functional state or federal regulator).

**Massachusetts** law provides that 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 Massachusetts' security breach notification law "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

require additional notice to the state.

Even where notice to individuals of a security breach is not required because the breach is unlikely to harm consumers, four states—**Alaska**,<sup>68</sup> **Florida**,<sup>69</sup> **South Dakota**,<sup>70</sup> and **Vermont**<sup>71</sup> — require notice to state agencies of this determination. **Alaska** requires notice to the Attorney General if, after an appropriate investigation, 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.<sup>72</sup> **Florida** requires that if notice to consumers is not sent because, after “an appropriate investigation and consultation with relevant federal, state, or local law enforcement agencies, the covered entity reasonably determines that the breach has not and will not likely result in identity theft or any other financial harm to the individuals whose personal information has been accessed,” the determination must be documented in writing and provided to the Department of Legal Affairs within 30 days after the determination. Under **South Dakota** law, notice to the Attorney General, but not consumers, is required “if, following an appropriate investigation . . . the information holder reasonably determines that the breach will not likely result in harm to the affected person.”<sup>73</sup> **Vermont** requires notice to the Attorney General or department of financial regulation of any determination that notice to consumers is not required. Notice to consumers is not required if a data collector “establishes” that “misuse of personal information is not reasonably possible.” This determination, however, must be sent with “a detailed explanation” to the Vermont Attorney General or the depart-

---

consumer affairs and business regulation of the breach as soon as practicable and without unreasonable delay following the breach.” Mass. Gen. Laws Ann. ch. 93H, § 5. 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 the person or agency has taken or plans to take relating to the breach pursuant to the applicable federal law, rule, regulation, guidance or guidelines. *Id.*

<sup>68</sup>Alaska Stat. § 45.48.010(c).

<sup>69</sup>Fla. Stat. Ann. § 501.171(4)(c).

<sup>70</sup>S.D. Codified Laws § 22-40-20.

<sup>71</sup>Vt. Stat. Ann. tit. 9, § 2435(d)(1).

<sup>72</sup>Alaska Stat. § 45.48.010(c).

<sup>73</sup>S.D. Codified Laws § 22-40-20.

ment of financial regulation.<sup>74</sup> Florida and Alaska require that written documentation of the basis for not providing notice be maintained for five years, while South Dakota requires retention for only three years. Under Alaska law, this notification is not considered a public record open to inspection by the public.<sup>75</sup> Under Vermont law, this notice may be, but is not automatically, treated confidentially.<sup>76</sup> **Alabama** adopted the requirement that a determination by a covered entity that notice to consumers is not required must be documented in writing and maintained for five years, but did not also require notice to a state agency.<sup>77</sup> **Louisiana** enacted a similar requirement, except that it also provides that, if requested, the documentation must be provided to the Attorney General within 30 days of the request.<sup>78</sup> **Maryland**<sup>79</sup> and **South Dakota**<sup>80</sup> impose three year retention periods, and **Alabama**,<sup>81</sup> **Alaska**,<sup>82</sup> **Florida**,<sup>83</sup> **Iowa**,<sup>84</sup> **Louisiana**,<sup>85</sup> **Missouri**,<sup>86</sup> **New Jersey**<sup>87</sup> and **Oregon**<sup>88</sup> require five years.

**Idaho** provides that where an agency becomes aware of a breach, regardless of whether notice is required, the Idaho Attorney General must be given notice within 24 hours of

---

<sup>74</sup>Vt. Stat. Ann. tit. 9, § 2435(d)(1).

<sup>75</sup>Alaska Stat. § 45.48.010(c).

<sup>76</sup>The communication may be designated as “trade secret” and treated confidentially if applicable. *See* Vt. Stat. Ann. tit. 9, § 2435(d)(1). If a data collector subsequently determines that misuse in fact has occurred or is occurring, however, it must provide notice to consumers as otherwise required by Vermont law. *Id.* § 2435(d)(2).

<sup>77</sup>*See* Ala. Code § 8-38-5(f).

<sup>78</sup>*See* La. Rev. Stat. Ann. § 51:3074(I).

<sup>79</sup>Md. Code Ann., Com. Law § 14-3504(b)(4). A *record* is defined under Maryland law as “information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.” *Id.* § 14-3501(f).

<sup>80</sup>S.D. Codified Laws § 22-40-20.

<sup>81</sup>Ala. Code § 8-38-5(f).

<sup>82</sup>Alaska Stat. § 45.48.010(c).

<sup>83</sup>Fla. Stat. Ann. § 501.171(4)(c).

<sup>84</sup>Iowa Code Ann. § 715C.2(6).

<sup>85</sup>La. Rev. Stat. Ann. § 51:3074(I).

<sup>86</sup>Mo. Rev. Stat. § 407.1500.2(5).

<sup>87</sup>N.J. Stat. Ann. § 56:8-163(a).

<sup>88</sup>Ore. Stat. § 646A.604(6).

discovery of the breach.<sup>89</sup>

Notices sent to state agencies generally are public documents. Some jurisdictions post notice letters on their websites.

Attorneys providing notice to state Attorneys General or agencies should anticipate further inquiries (and in some cases calls or letters informally seeking additional information or potentially even a subpoena compelling production of documents). Where a security breach involves a hacking attack, for example, as opposed to the theft of data stored on a laptop or other physical media, an inquiry may be made about the nature of the breach and what remedial measures have been taken. Some requests may address local practice not apparent from the face of a statute. For example, **North Carolina** requires that a Security Breach Reporting Form be completed and the **Maryland** Attorney General's Office insists that a copy of the actual notice to consumers be provided. Where a state statute does not require that a copy of the notice to consumers be provided (or where notice to a state agency must be provided prior to notice being sent to consumers), regulators nonetheless may request copies of the actual notices sent to consumers. In addition, **Massachusetts** law expressly contemplates that the director of consumer affairs and business relations will identify consumer reporting and/or state agencies that must be sent additional notices (as discussed in a footnote earlier in this subsection).

Communications with state regulators may or may not be treated confidentially. Under **Florida** law, for example, information received by the Department of Legal Affairs pursuant to a notification required by Florida's security breach notification statute, or received pursuant to an investigation by the department or a law enforcement agency, is treated as confidential and is exempt from disclosure under Florida law, but only until such time as the investigation is completed or ceases to be active.<sup>90</sup> Communications to regulators therefore potentially could be used in civil litigation or

---

<sup>89</sup>Idaho Code Ann. § 28-51-105.

<sup>90</sup>Fla. Stat. Ann. § 501.171(11)(a). During an investigation, information otherwise confidential may be disclosed:

1. In the furtherance of its official duties and responsibilities;
2. For print, publication, or broadcast if the department determines that such release would assist in notifying the public or locating or

obtained by reporters and reprinted in the press or online.

If the breach or harm to consumers is significant, one or more state Attorneys General also may initiate formal investigations or take legal action. If this is the case, a person or entity required to provide notice may want to consider offering credit monitoring services as a way to mitigate the impact of the breach.<sup>91</sup>

### **27.08[9] The Provision of Credit Monitoring Services to Affected Consumers**

Credit reporting agencies and other companies offer various different identity theft prevention and mitigation services, such as credit monitoring, that businesses may purchase for consumers adversely affected by a breach or that consumers may purchase for themselves. As of early 2019, only Connecticut and Delaware required that “identity theft prevention and mitigation” services, such as credit monitoring services, be purchased as a matter of course in response to a security breach<sup>1</sup> (although, as noted below, California and Oregon law requires that specific notices be provided if these services are offered). Whether or not required to do so, many companies elect to provide credit monitoring or similar services to affected customers, employ-

---

identifying a person that the department believes to be a victim of a data breach or improper disposal of customer records, except that information made confidential and exempt by paragraph (c) may not be released pursuant to this subparagraph; or

3. To another governmental entity in the furtherance of its official duties and responsibilities.

*Id.* § 501.171(11)(b). Upon completion of an investigation, or once an investigation ceases to be active, the following information received by the department shall remain confidential and generally exempt from disclosure:

1. All information to which another public records exemption applies.
2. Personal information.
3. A computer forensic report.
4. Information that would otherwise reveal weaknesses in a covered entity’s data security.
5. Information that would disclose a covered entity’s proprietary information.

*Id.* § 501.171(11)(c).

<sup>91</sup>*See infra* § 27.08[9].

#### **[Section 27.08[9]]**

<sup>1</sup>*See* Conn. Gen. Stat. Ann. § 36a-701b(b)(2)(B); Del. Code Ann. tit. 6, § 12B-102(e); Or. Rev. Stat. Ann. § 646A.604(7).

ees or other users as a goodwill gesture, and to encourage customer loyalty, in the event of a breach. In addition, state Attorneys General may require that credit monitoring services be provided to consumers for a period of time (typically one, two or three years) as part of the settlement of an enforcement action, depending on the nature and severity of the breach. Credit monitoring services are also sometimes sought as a remedy, or claimed as damages, by plaintiffs in litigation and often are purchased by plaintiffs in putative class action suits to allege injury for purposes of establishing standing in a federal court cases arising out of a security breach.<sup>2</sup> Accordingly some businesses choose to voluntarily provide credit monitoring services to deprive potential plaintiffs of the ability to claim a compensable injury to establish standing in a security breach case where, despite the breach, no financial loss to individual consumers has occurred.<sup>3</sup>

Credit monitoring or identity theft prevention or mitigation services are only useful for certain types of breaches. Credit monitoring services can be helpful in mitigating risk, for example, when a breach has exposed a Social Security Number that a hacker could use to open a bank account or apply for a new credit card, lease a car, or seek a loan. By contrast, where only a credit card number has been exposed, a hacker generally would not be able to obtain new credit by using only that information. A credit card number could be used to make unauthorized charges until it is cancelled, but those charges would appear on a customer's own credit card statement (or be available online).

If a business elects to provide credit monitoring services, it should include information about the service in its notice letter to consumers (assuming that it can do so without delaying notice in the time required by applicable statutes) or in a

---

<sup>2</sup>See generally *supra* § 27.07 (analyzing case law).

<sup>3</sup>See *supra* § 27.07 (analyzing cases). The Seventh Circuit has held that a company's decision to offer credit monitoring following a security breach may evidence that the risk of harm was more than *de minimis*, and therefore may confer standing to sue in federal court on a plaintiff who was provided with credit monitoring services following a breach. See *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688, 693-94 (7th Cir. 2015); see also *Galaria v. Nationwide Mutual Insurance Co.*, 663 F. App'x 384 (6th Cir. 2016) (adopting the same analysis in an unreported, 2-1 decision); see generally *supra* § 27.07 (criticizing this analysis and outlining a suggested approach for companies).

subsequent communication. It should also mention this fact in communications with state Attorneys General.<sup>4</sup>

While not required, **California** provides that *if* identity theft prevention and mitigation services are offered, and if the person or business providing notification was the source of the breach, then the offer to provide identity theft prevention and mitigation services must be included in the notice to any person whose information was or may have been breached if the breach exposed personal information (as defined under the California security breach notification law) and the notice must state that it will be provided at no cost to the affected person for not less than 12 months, and provide the information necessary to take advantage of the offer.<sup>5</sup> This odd formulation—requiring specific disclosures and a time period *if* identity theft prevention and mitigation services are offered, without expressly requiring that these services be offered—represented a legislative compromise that was reached at the time California’s security breach notification law was amended in 2014 to address this issue.

**Oregon**, like California, adopted disclosure rules in 2018 in the event credit monitoring or identity theft and prevention services are offered following a breach, but does not require that these services be offered. If a person must notify a consumer of a breach of security and, in connection with the notification, offers to provide credit monitoring services or identity theft prevention and mitigation services without charge to the consumer, then Oregon law provides that the person may not condition those services on the consumer’s providing the person with a credit or debit card number or on the consumer’s acceptance of any other service the person offers to provide for a fee.<sup>6</sup> Conversely, if a person offers additional credit monitoring services or identity theft prevention and mitigation services for a fee, that person must “separately, distinctly, clearly and conspicuously disclose in the offer for the additional credit monitoring services or identity theft prevention and mitigation services that the person will charge the consumer a fee.”<sup>7</sup> Oregon law further provides that the terms and conditions of any contract under which one person offers or provides credit monitoring ser-

---

<sup>4</sup>See *supra* § 27.08[8].

<sup>5</sup>Cal. Civ. Code § 1798.82(d)(2)(H).

<sup>6</sup>Or. Rev. Stat. Ann. § 646A.604(7)(a).

<sup>7</sup>Or. Rev. Stat. Ann. § 646A.604(7)(b).

vices or identity theft prevention and mitigation services on behalf of another person, in connection with notification of a security breach, must require compliance with the requirements set forth in this paragraph.<sup>8</sup>

Even though it is not required, it nevertheless may be prudent for companies to consider providing free identity theft mitigation and prevention services to California and Oregon residents (if not even more broadly) in circumstances where these services could mitigate the consequences of a potential breach because these statutory provisions may be cited by plaintiffs' class action lawyers as evidence of a reasonable practice in security breach litigation brought against companies that do not provide mitigation services to California residents.

In contrast to California and Oregon, Connecticut and Delaware affirmatively mandate provision of mitigation services.

The California law, with the equivocal language removed, was largely incorporated into **Connecticut's** security breach notification law in 2015 (and the Connecticut law was amended in 2018 to double the amount of time for which free services should be provided, to 24 months). Connecticut law provides that where a person is required to provide notice of a security breach to a Connecticut resident, that person must offer the affected resident (*i.e.*, someone whose personal information, as defined under the Connecticut security breach statute, was breached or was reasonably believed to have been breached) "appropriate identity theft prevention services and, if applicable, identity theft mitigation services."<sup>9</sup>

Theft prevention and, if applicable, mitigation services, must be provided to Connecticut residents whose personal information was breached (or is reasonably believed to have been breached), free of charge, for not less than 24 months.<sup>10</sup> The law also requires that notice of the availability of these services and information on placing a credit freeze on a consumer's credit file be provided, but not necessarily in the notice of breach.<sup>11</sup> Connecticut law further requires that "all information necessary" for affected residents to enroll in

---

<sup>8</sup>Or. Rev. Stat. Ann. § 646A.604(7)(c).

<sup>9</sup>Conn. Gen. Stat. Ann. § 36a-701b(b)(2)(B).

<sup>10</sup>Conn. Gen. Stat. Ann. § 36a-701b(b)(2)(B).

<sup>11</sup>See Conn. Gen. Stat. Ann. § 36a-701b(b)(2)(B).

identity theft prevention and, if applicable, mitigation services, along with information on how a resident can put a credit freeze on his or her credit file, be provided to affected residents.<sup>12</sup> As a practical matter, companies may find it more economical to include this information in the notice of breach to state residents—especially given that notice to the Connecticut Attorney General is required when security breach notification is provided to Connecticut residents.<sup>13</sup> On the other hand, if for some reason a company prefers to supply this information separately (for example, if appropriate services have not yet been secured by the time notice must be sent, or if there is concern about including this information in a letter to residents of one state but not others), Connecticut law appears to allow this.

**Delaware** followed Connecticut's lead in providing that, effective on or after April 14, 2018, if the security of personal information, including a social security number of a state resident, was breached or was "reasonably believed to have been breached, . . ." the resident must be provided with credit monitoring services at no cost to the resident for a period of one (1) year<sup>14</sup> (as well as all information necessary to enroll in a credit monitoring service and details on how to place a credit freeze on the resident's credit file).<sup>15</sup> These services are not required, however, "if, after an appropriate investigation, the person reasonably determines that breach of security is unlikely to result in harm to the individuals whose personal information has been breached."<sup>16</sup>

### **27.08[10] Claims, Defenses, Remedies and Sanctions for Non-compliance with Security Breach Notification Laws**

#### **27.08[10][A] In General**

States and territories differ widely in the remedies available in the event of noncompliance with their security breach notification statutes. Different jurisdictions authorize or

---

<sup>12</sup>See Conn. Gen. Stat. Ann. § 36a-701b(b)(2)(B).

<sup>13</sup>See Conn. Gen. Stat. Ann. § 36a-701b(b)(2)(A); *see generally supra* § 27.08[8] (analyzing notification obligations to state agencies, including state attorneys general).

<sup>14</sup>Del. Code Ann. tit. 6, § 12B-102(e).

<sup>15</sup>Del. Code Ann. tit. 6, § 12B-102(e).

<sup>16</sup>Del. Code Ann. tit. 6, § 12B-102(e).

proscribe private causes of action, while others are silent and may or may not allow such claims. As discussed in subsection 27.08[10][B], many states provide for enforcement by the Attorney General or other state officials. Businesses or individuals may be subject to widely varying statutory fines or damages, depending on the jurisdiction. Claims against state agencies are not uniformly authorized even in states that otherwise allow claims against persons or entities.

The security breach statutes in a small number of jurisdictions contain no express remedy provisions.<sup>1</sup>

**Ohio** has created an affirmative defense for a covered entity that creates, maintains, and complies with a written cybersecurity program, which may protect a covered entity from certain tort actions brought in Ohio state courts or under Ohio law.<sup>2</sup>

The **California** statute provides that any customer injured by a violation of the statute may institute a civil action to recover damages<sup>3</sup> or injunctive relief,<sup>4</sup> in addition to any other remedies that may be available.<sup>5</sup> Among other things, the breach of the notification statute itself could be actionable as an unfair trade practice under California law if damages can be shown.<sup>6</sup> Absent any injury traceable to a company's failure to reasonably notify customers of a data breach, a plaintiff may not have standing to bring suit, at least in federal court.<sup>7</sup>

Effective January 1, 2020, the California Consumer

---

[Section 27.08[10][A]]

<sup>1</sup>These jurisdictions include **Georgia** and **New Jersey**.

<sup>2</sup>See Ohio Rev. Code Ann. §§ 1354.01 to 1354.05; see generally *supra* § 27.04[6][H].

<sup>3</sup>Cal. Civil Code § 1798.84(b).

<sup>4</sup>Cal. Civil Code § 1798.84(e).

<sup>5</sup>Cal. Civil Code §§ 1798.84(g).

<sup>6</sup>See Cal. Bus. & Prof. Code §§ 17200 *et seq.*; see generally *supra* §§ 27.01, 27.04[6] (discussing how the breach of an unrelated statute may be actionable under § 17200).

<sup>7</sup>See, e.g., *In re Adobe Systems, Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1210–19 (N.D. Cal. 2014) (holding that plaintiffs lacked standing to assert a claim under Cal. Civil Code § 1798.82 for failing to provide reasonable notification to customers of a security breach as required by that statute); see generally *supra* § 27.07 (analyzing claims raised in security breach litigation).

Privacy Act (CCPA)<sup>8</sup> will authorize statutory damages of between \$100 and \$750 “per consumer per incident or actual damages, whichever is greater, injunctive or declaratory relief, and any other relief that a court deems proper.”<sup>9</sup> The CCPA creates a private right of action for consumers “whose nonencrypted or nonredacted personal information . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business’s violation of the duty to implement and maintain reasonable security procedures and practices . . . .”<sup>10</sup> The private right of action created by the CCPA may be brought only for data breaches arising from a business’s failure to maintain reasonable security measures, and not any other failures to comply with the

---

<sup>8</sup>Cal. Civ. Code §§ 1798.100 to 1798.199.

<sup>9</sup>Cal. Civ. Code § 1798.150(a)(1).

<sup>10</sup>Cal. Civ. Code § 1798.150(a)(1). *Personal information* in this section is defined by reference section 1798.81.5, which is narrower in scope than the CCPA’s definition in section 1798.140(o). *Personal information* under section 1798.81.5 means either of the following:

- (A) An individual’s first name or first initial and his or her last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:
  - (i) Social security number.
  - (ii) Driver’s license number or California identification card number.
  - (iii) 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.
  - (iv) Medical information.
  - (v) Health insurance information.
- (B) A username or email address in combination with a password or security question and answer that would permit access to an online account.

Cal. Bus. & Prof. Code § 1798.81.5(d)(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.” *Id.* § 1798.81.5(d)(4).

*Medical information* means any individually identifiable information, in electronic or physical form, regarding the individual’s medical history or medical treatment or diagnosis by a health care professional. *Id.* § 1798.81.5(d)(2).

*Health insurance information* means an individual’s insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual’s application and claims history, including any appeals records. *Id.* § 1798.81.5(d)(3).

CCPA.<sup>11</sup> In assessing the amount of statutory damages, courts will be directed to consider “any one or more of the relevant circumstances presented by any of the parties to the case, including, but not limited to, the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant’s misconduct, and the defendant’s assets, liabilities, and net worth.”<sup>12</sup> This provision, and the CCPA in general, are analyzed extensively in section 26.13A. A copy of the CCPA is reprinted in Appendix 8 to Chapter 26.

Remedies for the underlying security breach (as opposed to violation of a notification statute) may arise under state contract or tort law, civil statute or criminal law, as addressed in sections 27.07 and 46.09, and generally are not addressed in security breach notification statutes (except in Nevada). In addition, **Maine** makes it a violation of its security breach notification statute for an unauthorized person to release or use an individual’s personal information acquired through a security breach.<sup>13</sup>

Special rules governing liability to financial institutions for breaches of credit and debit card information, and potential defenses, are separately analyzed in section 27.08[14].

Subsections 27.08[10][B] and 27.08[10][C] address, respectively, state enforcement of security breach notification laws and private causes of action.

### **27.08[10][B] State Enforcement**

A large number of jurisdictions provide for state enforcement of security breach notification statutes, often as an unfair trade practice.

**Alaska** provides for enforcement against information collectors that are government agencies when notice is not provided, with civil penalties of \$500 per resident who did not receive notice, to a maximum of \$50,000, plus injunctive

---

<sup>11</sup>Cal. Civ. Code § 1798.150(c).

<sup>12</sup>Cal. Civ. Code § 1798.150(a)(2).

<sup>13</sup>Me. Rev. Stat. Ann. tit. 10, § 1347-A.

relief.<sup>1</sup>

**Illinois** makes a violation of its statute unlawful under its Consumer Fraud and Deceptive Business Practices Act,<sup>2</sup> as does **Pennsylvania** under its Unfair Trade Practices and Consumer Protection Law.<sup>3</sup> In **Connecticut**, **Mississippi** and **Washington** it is deemed an unfair trade practice, enforced by the Attorney General.<sup>4</sup> In **Iowa** it is an unlawful practice enforced by the Attorney General, but the Attorney General may seek and obtain an order that a party held to have violated the statute pay damages to the Attorney General on behalf of an injured person.<sup>5</sup> Under **Kansas** law, violations of the security breach notification statute (except by insurance companies licensed to do business in the state) may be enforced by the Attorney General, although the statute makes clear that this provision is not exclusive and does not relieve an individual or a commercial entity from compliance with all other applicable law.<sup>6</sup> **Arkansas**,<sup>7</sup> **Massachusetts**,<sup>8</sup> **Minnesota**,<sup>9</sup> **North Dakota**,<sup>10</sup> **Rhode Island**<sup>11</sup> and **Ohio**<sup>12</sup> likewise authorize enforcement by their respective attorneys general. The exact remedies, however, are not

[Section 27.08[10][B]]

<sup>1</sup>Alaska Stat. § 45.48.080.

<sup>2</sup>See 815 Ill. Comp. Stat. Ann. 530/20.

<sup>3</sup>See 73 Pa. Stat. Ann. § 2308.

<sup>4</sup>Conn. Gen. Stat. Ann. § 36a-701b(g); Miss. Code Ann. § 75-24-29(8); Wash. Rev. Code Ann. § 19.255.010(17).

<sup>5</sup>Iowa Code Ann. § 715C.2(8)(a). The rights and remedies under this statute are cumulative to each other and to any other rights and remedies available under the law. Iowa Code Ann. § 715C.2(8)(a).

<sup>6</sup>Kan. Stat. Ann. § 50-7a02(g).

<sup>7</sup>Ark. Code Ann. § 4-110-108.

<sup>8</sup>Mass. Gen. L. Ann. ch. 93H, § 6 (“The attorney general may bring an action pursuant to section 4 of chapter 93A against a person or otherwise to remedy violations of this chapter and for other relief that may be appropriate.”); Mass. Gen. L. Ann. ch. 93A, §§ 2, 4.

<sup>9</sup>See Minn. Stat. Ann. § 325E.61(6).

<sup>10</sup>N.D. Cent. Code § 51-30-07.

<sup>11</sup>R.I. Gen. Laws § 11-49.3-5.

<sup>12</sup>Ohio Rev. Code §§ 1347.12(G), 1347.19(I), 1349.191, 1349.192. The Attorney General is authorized to seek civil penalties for non-compliance. See Ohio Rev. Code §§ 1347.12(G), 1347.19(I), 1349.191, 1349.192. As noted later in this section, Ohio also provides a potential safe harbor defense in litigation for covered entities that adopt and adhere to written cybersecurity information programs from certain tort claims arising out of

specified and these states do not expressly provide that a violation is deemed to be an unfair trade practice.

For violations by insurance companies licensed to do business in the state, **Kansas** law provides that the insurance commissioner shall have the sole authority to enforce violations of the state's security breach notification statute.<sup>13</sup>

In **Indiana** a violation is deemed a deceptive act actionable only by the Attorney General subject to civil penalty of up to \$150,000 per deceptive act (with the caveat that the failure to provide notice in connection with a "related series of breaches" will be treated as merely a single deceptive act).<sup>14</sup> **Iowa** deems a violation to be an unlawful practice and provides that in addition to the remedies available for unlawful practices, the Attorney General may seek and obtain an order that the party held to violate the security breach notification statute pay damages to the Attorney General on behalf of a person injured by the violation.<sup>15</sup> **West Virginia** similarly defines the failure to comply with notice provisions as an unfair or deceptive act or practice enforceable exclusively by the Attorney General, but further provides that no civil penalty may be assessed unless the court finds that the defendant engaged in "a course of repeated and willful violations" (in which case a penalty of up to \$150,000 may be assessed "per breach of the security system or series of breaches of a similar nature that are discovered in a single investigation.").<sup>16</sup>

**Vermont** provides that the state Attorney General and state's attorney "have sole and full authority" to "investigate[,] . . . enforce, prosecution, obtain and impose remedies" under the statute (except for data collectors licensed or registered with the department of banking, insurance, securities and health care administration, which has similar jurisdiction over such persons and entities).<sup>17</sup> Thus, in Vermont, a violation could result in a civil unfair competition suit brought by the Attorney General, a criminal action brought by the state's attorney or an action brought by other

---

a security breach.

<sup>13</sup>Kan. Stat. Ann. § 50-7a02(h).

<sup>14</sup>See Ind. Code § 24-4.9-4-1; 24-4.9-4-2.

<sup>15</sup>Iowa Code Ann. § 715C.2(8).

<sup>16</sup>W. Va. Code § 46-2A-104.

<sup>17</sup>See Vt. Stat. Ann. tit. 9, § 2435(g).

regulators. The Attorney General also has authority to enforce Vermont's data broker registration and information security law provisions, the violation of which would be deemed an unfair and deceptive act under Vermont law.<sup>18</sup>

Some states provide for enforcement by the Attorney General, but without expressly deeming a violation of the statute an unfair trade practice. For example, **Colorado**<sup>19</sup> and **Wyoming**<sup>20</sup> provide that the Attorney General may bring an action in law or equity to address violations of the statute and for other relief that may be appropriate to ensure compliance or to recover direct economic damages (or damages under Wyoming statute) resulting from a violation, or both. This provision, however, is not exclusive and does not relieve an individual or commercial entity from compliance with other applicable laws. Colorado's law allows for enforcement of both its security breach notification law and its statute requiring businesses to maintain reasonable security precautions.<sup>21</sup>

Like Vermont, Colorado also makes provision for criminal, in addition to civil, enforcement.<sup>22</sup>

**Alabama**'s security breach notification law does not provide for a private cause of action but grants the Attorney General exclusive authority to sue, in a representative capacity on behalf of those affected, to recover \$5,000 per day per violation to a maximum of \$500,000.<sup>23</sup> It also provides that a violation of the notification law is deemed a violation of Alabama's Deceptive Trade Practices Act.<sup>24</sup> The statute also contemplates a mechanism for covered entities and third party agents to obtain a reprieve from the obligation to provide notice by stating that it is not a violation of the act to refrain from providing any notice required under the security breach notification law if a court of competent jurisdic-

---

<sup>18</sup>See Vt. Stat. Ann. tit. 9, § 2447(d); *see generally supra* § 27.04[6][J].

<sup>19</sup>Colo. Rev. Stat. Ann. § 6-1-716(4).

<sup>20</sup>Wyo. Stat. Ann. § 40-12-502(f).

<sup>21</sup>See Colo. Rev. Stat. Ann. §§ 6-1-713.5, 6-1-716(4).

<sup>22</sup>See Colo. Rev. Stat. Ann. §§ 6-1-716(5), 18-5.5-102; Vt. Stat. Ann. tit. 9, § 2435(g).

<sup>23</sup>Ala. Code § 8-83-9.

<sup>24</sup>Ala. Code § 8-83-9(a).

tion has directed otherwise.<sup>25</sup>

**Arizona's** statute provides that it may be enforced exclusively by the Attorney General, who may bring an action for willful and knowing violations of the statute to recover actual damages and a civil penalty of up to \$10,000 per breach or series of breaches of a similar nature that are discovered in a single investigation.<sup>26</sup>

The **District of Columbia** provides that the Attorney General may petition for temporary or permanent injunctive relief and for an award of restitution for property lost or damages suffered by D.C. residents as a consequence of a violation of the D.C. security breach notification statute. The Attorney General may also recover a civil penalty of up to \$100 per violation (with each failure to provide a D.C. resident with notification constituting a separate violation), the costs of the action and reasonable attorneys' fees. D.C. residents are also authorized to institute civil actions to recover actual damages (excluding "dignitary damages, including pain and suffering"), costs and reasonable attorneys' fees. These remedies are cumulative to each other and any other rights or remedies available under law.<sup>27</sup>

Under **Hawaii** law, a business (but not a government entity) that violates the statute may be liable for penalties of up to \$2,500 per violation in an action brought by the Attorney General or the Executive Director of the Office of Consumer Protection.<sup>28</sup> Hawaii law also authorizes a private cause of action by the injured party for damages against a business (but not a government entity) that violates the statute. In such an action, a court may award reasonable attorneys' fees to the prevailing party.<sup>29</sup>

**Michigan** provides that a person (or entity) that knowingly fails to provide notice under the statute may be ordered to pay a civil fine of not more than \$250 for each failure to provide notice in an action brought by the Attorney General.<sup>30</sup> The aggregate liability for civil fines arising from the same

---

<sup>25</sup>Ala. Code § 8-83-9(b)(3).

<sup>26</sup>Ariz. Rev. Stat. § 18-552(H).

<sup>27</sup>D.C. Stat. § 28-3853.

<sup>28</sup>Haw. Rev. Stat. Ann. § 487N-3 (b).

<sup>29</sup>Haw. Rev. Stat. Ann. § 487N-3(a).

<sup>30</sup>Haw. Rev. Stat. Ann. § 445.72(13).

security breach, however, may not exceed \$750,000.<sup>31</sup> These provisions, however, do not affect the availability of any civil remedy for a violation of state or federal law.<sup>32</sup>

**Missouri** authorizes the Attorney General to bring an action to recover actual damages for “a willful and knowing violation” of its security breach notification statute and recover a civil penalty of up to \$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.”<sup>33</sup>

A violation of **Oklahoma’s** statute applicable to security breaches by individuals and entities may be enforced by the Attorney General or a district attorney in the same manner as an unlawful practice under the Oklahoma Protection Act. Violations by state-chartered or state-licensed financial institutions are enforceable exclusively by the primary state regulator of the financial institution. Other than this exception, the Attorney General or a district attorney have exclusive authority to bring an action to recover either actual damages for a violation of the statute or a civil penalty of up to \$150,000 per breach or series of breaches of a similar nature that are discovered in a single investigation.<sup>34</sup>

**Nebraska** authorizes its Attorney General to “issue subpoenas and seek and recover direct economic damages for each affected Nebraska resident injured by a violation” of its notification statute. Nebraska law also provides that a violation of its security breach notification law constitutes a violation of its Consumer Protection Act.<sup>35</sup>

**New York** authorizes its Attorney General to bring an action in the name and on behalf of the people of New York for preliminary relief, damages for actual costs or losses, including consequential financial losses. In addition, if a court determines that a person or business violated the statute knowingly or recklessly the court may impose a civil penalty in the amount of the greater of \$5,000 or up to \$10 per instance of failed notification to a maximum of \$150,000.

**New Hampshire** includes similar provisions, but for civil actions. The Attorney General’s Office is authorized to

---

<sup>31</sup>Haw. Rev. Stat. Ann. § 445.72(14).

<sup>32</sup>Haw. Rev. Stat. Ann. § 445.72(15).

<sup>33</sup>Mo. Rev. Stat. § 407.1500.4.

<sup>34</sup>Okla. Stat. Ann. tit. 24, § 165.

<sup>35</sup>Neb. Rev. Stat. § 87-806.

enforce the security breach notification statute. In addition, any person injured by a violation may bring an action for damages and equitable relief (and need not post a bond to obtain injunctive relief, subject to the discretion of the court). A prevailing plaintiff will be entitled to actual damages, however where an act or practice was found to constitute a willful or knowing violation the court must award up to treble damages but not less than double damages. A prevailing plaintiff shall also be awarded the costs of the suit and reasonable attorneys' fees. Any attempted waiver of the right to the damages provisions set forth in the statute will be deemed void and unenforceable. In addition, under New Hampshire law, the burden is on the party responsible for complying with the security breach notification statute to demonstrate its compliance.<sup>36</sup>

**New Mexico** authorizes its Attorney General to bring an action on behalf of individuals in the name of the state, when the Attorney General "has a reasonable belief that a violation" of the security breach notification statute has occurred. The Attorney General potentially may obtain (a) an injunction, (b) actual costs or losses, including consequential financial losses, or (c) if the court determines that a defendant violated the act "knowingly or recklessly, the court may impose a civil penalty of the greater of twenty-five thousand dollars (\$25,000) or, in the case of failed notification, ten dollars (\$10.00) per instance of failed notification up to a maximum of one hundred fifty thousand dollars (\$150,000)."<sup>37</sup>

**South Dakota** provides for enforcement by the Attorney General as a deceptive act or practice pursuant to S.D. Codified Laws § 37-24-6. In addition to any other remedy authorized under that law, the Attorney General may recover a civil penalty of not more than \$10,000 per day per violation. The Attorney General is also authorized to recover attorneys' fees.<sup>38</sup>

**Texas** authorizes its Attorney General recover a civil penalty of up to \$100 for each individual to whom notification should have been sent "for each consecutive day that the person fails to take reasonable action to comply" with

---

<sup>36</sup>See N.H. Rev. Stat. Ann. § 359-C:21.

<sup>37</sup>N.M. Stat. Ann. § 57-12C-11.

<sup>38</sup>See S.D. Codified Laws § 22-40-25.

the subsection to a maximum of \$250,000 for each violation, injunctive and other equitable relief, costs and reasonable attorneys' fees.<sup>39</sup> This provision allows a fair amount of discretion to both companies and prosecutors (although businesses would be well advised to move quickly). Texas law does not provide a specific time frame within which notice must be given. Rather, it merely requires a person send notice "as quickly as possible," except when a law enforcement agency determines that notification would impede a criminal investigation (at which point it must be given "as soon as the law enforcement agency determines that the notification will not compromise the investigation") or "as necessary to determine the scope of the breach and restore the reasonable integrity of the data system."<sup>40</sup>

**Utah's** statute is likewise enforceable by the Attorney General, who may seek injunctive relief and attorneys' fees and/or up to \$2,500 per consumer (regardless of the number of violations) to a maximum of \$100,000 for related violations (regardless of the number of affected consumers).<sup>41</sup>

**Guam** and **Virginia** allow enforcement by the Attorney General and authorizes a civil penalty of up to \$150,000 per breach. In addition, the availability of this remedy does not limit an individual from recovering direct economic damages from a violation of the statute.<sup>42</sup> However, a violation by a state-chartered or licensed financial institution may be enforced exclusively by the financial institution's primary state regulator and a violation by a person or entity regulated by the State Corporation Commission's Bureau of Insurance may be enforced exclusively by the State Corporation Commission.<sup>43</sup>

Other jurisdictions provide for enforcement by state authorities other than the Attorney General. For example, in **Idaho** a breach of the statute may be enforced by the primary regulator of a business, which may recover up to \$25,000 per breach if an agency, individual or commercial entity intentionally fails to give notice required by the

---

<sup>39</sup>Tex. Bus. & Comm. Code § 521.151.

<sup>40</sup>Tex. Bus. & Comm. Code §§ 521.053(b), 521.053(d); Tex. Gov't Code §§ 205.010, 2054.1125 (applying section 521.053(b) to state and local governments).

<sup>41</sup>Utah Code Ann. § 13-44-301.

<sup>42</sup>See 9 Guam Code Ann. § 48.50; Va. Code Ann. § 18.2-186.6(I).

<sup>43</sup>Va. Code Ann. § 18.2-186.6(J), 18.2-186.6(K).

statute.<sup>44</sup> **Maine** similarly provides for enforcement by the Department of Financial Regulation or the Attorney General and authorizes fines of not more than \$500 per violation (to a maximum of \$2,500 per day for each day an information broker is in violation of the law), equitable relief and/or enjoinder from further violations.<sup>45</sup>

Maine also makes it a violation of its security breach notification statute for an unauthorized person to release or use an individual's personal information acquired through a security breach.<sup>46</sup>

Violations of **Oregon's** law may be enforced by the Director of the Department of Consumer and Business Services and may result in a penalty of up to \$1,000 per day per violation to a maximum of \$500,000.<sup>47</sup> **Puerto Rico** authorizes fines of \$500 to a maximum of \$5,000 for each violation of the security breach statute or regulations. The fines provided for in the statute do not affect the rights of consumers to initiate actions or claims for damages.<sup>48</sup>

**South Carolina** authorizes an administrative fine of up to \$1,000 for each resident whose information was accessible by virtue of a security breach, in an amount to be determined by the Department of Consumer Affairs, in cases where an agency or person acts knowingly and willfully in violating the security breach notification statute.<sup>49</sup> South Carolina also authorizes a private cause of action for damages, an injunction to enforce compliance and attorneys' fees for residents who are injured by a violation of the statute by persons or state agencies, in addition to and cumulative of all other rights and remedies available.<sup>50</sup>

In **Florida**, the Department of Legal Affairs is authorized to sue covered entities and third-party agents that fail to provide required notices as an unfair or deceptive trade practice.<sup>51</sup> In addition, a covered entity's failure to provide notice to consumers and the Department of Legal Affairs

---

<sup>44</sup>See Idaho Code Ann. § 28-51-107.

<sup>45</sup>See Me. Rev. Stat. Ann. tit. 10, § 1349.

<sup>46</sup>Me. Rev. Stat. Ann. tit. 10, § 1347-A.

<sup>47</sup>See Or. Rev. Stat. Ann. § 646A.624(4).

<sup>48</sup>P.R. Stat. Ann. § 4055.

<sup>49</sup>S.C. Code Ann. §§ 1-11-490(H) (agencies), 39-1-90(H) (persons).

<sup>50</sup>S.C. Code Ann. §§ 1-11-490(G) (agencies), 39-1-90(G) (persons).

<sup>51</sup>Fla. Stat. Ann. § 501.171(9)(a). A *covered entity* is "a sole proprietor-

within the time periods prescribed for providing notice may result in an administrative fine of \$1,000 per day for the first thirty days and thereafter \$50,000 for each subsequent thirty-day period (or portion thereof), up to a maximum of \$500,000.<sup>52</sup>

Florida also has made it unlawful for a person to intentionally or knowingly possess, without authorization, the personal identification information of another person in any form, including, but not limited to, mail, physical documents, identification cards, or information stored in digital form.<sup>53</sup>

Violations of **Montana's**<sup>54</sup> notification statute may be enforced as an unfair trade practice by the Montana Department of Justice.

In **Rhode Island**, reckless violations of the security breach notification statute may result in a civil penalty of up to \$100 per record and knowing and willful violations may lead to a civil penalty of up to \$200 per record (with no cap for either reckless or knowing and willful violations).<sup>55</sup>

**Nevada** narrowly authorizes enforcement by a temporary restraining order or permanent injunction.<sup>56</sup>

---

ship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity” and for some purposes a governmental entity, “that acquires, maintains, stores, or uses personal information.” *Id.* § 501.171(1)(b). A *governmental entity* is “any department, division, bureau, commission, regional planning agency, board, district, authority, agency, or other instrumentality of this state that acquires, maintains, stores, or uses data in electronic form containing personal information.” *Id.* § 501.171(1)(f). A *third-party agent* is “an entity that has been contracted to maintain, store, or process personal information on behalf of a covered entity or governmental entity.” *Id.* § 501.171(1)(h).

<sup>52</sup>See Fla. Stat. Ann. § 501.171(9)(b). While Ohio and Wisconsin also set outer limits of forty-five (45) days for compliance (which in Ohio is a firm deadline; see *supra* § 27.08[4]), their security breach notification statutes do not include parallel penalty provisions.

<sup>53</sup>Fla. Stat. Ann. § 817.5685. *Personal identification information* within the meaning of this statute means a person’s social security number, official state-issued or United States-issued driver license or identification number, alien registration number, government passport number, employer or taxpayer identification number, Medicaid or food assistance account number, bank account number, credit or debit card number, and medical records. *Id.* § 817.5685(1).

<sup>54</sup>Montana Code Ann. § 30-14-1705.

<sup>55</sup>See R.I. Gen. Laws § 11-49.3-5.

<sup>56</sup>See Nev. Rev. Stat. § 603A.920.

**27.08[10][C] Private Claims for Damages,  
Injunctive Relief and Attorneys' Fees**

Private causes of action may be permitted, prohibited or limited depending on applicable state law.

Private civil actions are expressly authorized under a number of statutes, including those enacted in **California**, the **District of Columbia**, **Hawaii**, **Michigan**, **New Hampshire**, **Puerto Rico** and **South Carolina**. **Delaware**, for example, provides that nothing in its security breach notification statute may be construed to modify any right which a person may have at common law, by statute or otherwise.<sup>1</sup>

**Alaska** allows suits for breach as an unfair or deceptive act or practice, but caps damages. In a suit against an information collector that is either a government agency or a private person or entity, the collector may be fined up to \$500 for each state resident who was not sent notice fined to a maximum of \$50,000. In a suit against an information collector that is a private person, actual economic damages of up to \$500 may also be awarded.<sup>2</sup>

**Oregon** provides that a violation of Oregon's security breach notification law is an unlawful practice under Oregon law.<sup>3</sup> Oregon also provides that the rights and remedies created by its security breach notification law "are cumulative and are in addition to any other rights or remedies that are available under law."<sup>4</sup>

Under **Louisiana** law, a civil action may be instituted for failing to disclose a breach "in a timely manner."<sup>5</sup> Likewise, under the laws of **Tennessee**, **Washington** and the **U.S. Virgin Islands**, any customer injured by a violation of the security breach notification statute may institute a civil action to recover damages or seek injunctive relief, in addition

---

**[Section 27.08[10][C]]**

<sup>1</sup>Del. Code Ann. tit. 6, § 12B-104(b).

<sup>2</sup>Alaska Stat. §§ 45.48.080, 45.50.531.

<sup>3</sup>Or. Rev. Stat. Ann. §§ 646A.604(9)(a), 646.607.

<sup>4</sup>Or. Rev. Stat. Ann. § 646A.604(9)(b).

<sup>5</sup>La. Stat. Ann. § 51:3075. The measure or basis for calculating damages is not spelled out in the statute.

to any other remedies that may be available.<sup>6</sup>

**Mississippi**<sup>7</sup> and **Kentucky**<sup>8</sup> provide that nothing in their respective security breach notification statutes may be construed to create a private right action. The **Utah** statute stipulates that nothing in the statute creates a private cause of action, although the statute likewise should not be read as affecting any private cause of action that otherwise may exist under other law, including contract and tort.<sup>9</sup> **North Carolina** states that a private cause of action may not be maintained unless an individual plaintiff has been injured as a result of the violation.<sup>10</sup> North Carolina law further provides that a cause of action may not be assigned.<sup>11</sup>

**Vermont** more specifically provides that the state Attorney General and state's attorney "have sole and full authority" to "investigate[,] . . . enforce, prosecut[e], obtain and impose remedies" under the statute (except for data collectors licensed or registered with the department of banking, insurance, securities and health care administration, which has similar jurisdiction over such persons and entities).<sup>12</sup> No private cause of action may be brought.

Like Vermont, **Florida**'s law states explicitly that there is no private cause of action, but it provides that in any action brought by the Department of Legal Affairs a violation of Florida's security breach notification statute by a covered entity or third-party agent shall be treated as an unfair or deceptive trade practice under Florida law.<sup>13</sup>

**Alabama** law similarly authorizes its Attorney General to file suit to enforce its security breach notification law as a deceptive trade practice, but provides that a violation of the

---

<sup>6</sup>See Wash. Code Ann. §§ 19.255.010(13) (persons and businesses), 42.56.590(12) (state agencies); V.I. Code Ann. tit. 14, § 2211.

<sup>7</sup>Miss. Code Ann. § 75-24-29(8).

<sup>8</sup>Ky. Rev. Stat. Ann. § 61.933(6).

<sup>9</sup>See Utah Code Ann. § 13-42-301.

<sup>10</sup>N.C. Gen. Stat. § 75-65(i).

<sup>11</sup>N.C. Gen. Stat. § 75-65(j).

<sup>12</sup>See Vt. Stat. Ann. tit. 9, § 2435(g). Vermont also authorizes the Attorney General to enforce its data broker registration and information security provisions. See Vt. Stat. Ann. tit. 9, § 2447(d); see generally *supra* § 27.04[6][J].

<sup>13</sup>Fla. Stat. Ann. §§ 501.171(9), 501.171(10). Definitions of *covered entities* and *third-party agents* may be found in section 27.08[10][B] and are not repeated here.

statute “does not establish a cause of action” for private entities or individuals,<sup>14</sup> although it also makes clear that nothing in the statute “may otherwise be construed to affect any right a person may have at common law, by statute, or otherwise.”<sup>15</sup>

**Nebraska** likewise provides that its security breach notification law “does not give rise to a private cause of action” (although the statute authorizes enforcement by the Attorney General).<sup>16</sup>

**Wisconsin** provides that the failure to comply with its notification statute “is not negligence or a breach of any duty, but may be evidence of negligence or breach of a duty.”<sup>17</sup>

**Ohio’s** cybersecurity law provides a defense to certain tort actions brought in Ohio state courts or under Ohio law that allege that the failure to implement reasonable information security controls resulted in a data breach.<sup>18</sup> The law creates an affirmative defense “to any cause of action sounding in tort” brought under Ohio law or in Ohio courts “that alleges that the failure to implement reasonable information security controls resulted in a data breach concerning personal information[,]” where a *covered entity*<sup>19</sup> has created, maintains, and complies with a written cybersecurity program

<sup>14</sup>Ala. Code § 8-38-9.

<sup>15</sup>Ala. Code § 8-38-9(a)(1).

<sup>16</sup>Neb. Rev. Stat. § 87-806.

<sup>17</sup>Wis. Stat. Ann. § 895(4).

<sup>18</sup>See Ohio Rev. Code Ann. §§ 1354.01 to 1354.05; see generally *supra* § 27.04[6][H]. A *data breach* means

unauthorized access to and acquisition of computerized data that compromises the security or confidentiality of personal information or restricted information owned by or licensed to a covered entity 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 person or property. “Data breach” does not include either of the following:

- (1) Good faith acquisition of personal information or restricted information by the covered entity’s employee or agent for the purposes of the covered entity’s, provided that the personal information or restricted information is not used for an unlawful purpose or subject to further unauthorized disclosure;
- (2) Acquisition of personal information or restricted information pursuant to a search warrant, subpoena, or other court order, or pursuant to a subpoena, order, or duty of a regulatory state agency.

Ohio Rev. Code Ann. § 1354.01(C).

<sup>19</sup>A *covered entity* means “a business that accesses, maintains, communicates, or processes personal information or restricted information in

that contains administrative, technical, and physical safeguards for the protection of personal information<sup>20</sup> (or

---

or through one or more systems, networks, or services located in or outside this state.” Ohio Rev. Code Ann. § 1354.01(B). A *business* is defined as “any limited liability company, limited liability partnership, corporation, sole proprietorship, association, or other group, however organized and whether operating for profit or not for profit, including a financial institution organized, chartered, or holding a license authorizing operation under the laws of this state, any other state, the United States, or any other country, or the parent or subsidiary of any of the foregoing.” *Id.* § 1354.01(A).

<sup>20</sup>*Personal information* has the same meaning as in section 1349.19 of the Revised Code. Ohio Rev. Code Ann. § 1354.01(D). Section 1349 defined *personal information* to mean

- (a) . . . an individual’s name, consisting of the individual’s first name or first initial and last name, in combination with and linked to any one or more of the following data elements, when the data elements are not encrypted, redacted, or altered by any method or technology in such a manner that the data elements are unreadable:
  - (i) Social security number;
  - (ii) Driver’s license number or state identification card number;
  - (iii) Account number or credit or debit card number, in combination with and linked to any required security code, access code, or password that would permit access to an individual’s financial account.
- (b) “Personal information” does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or any of the following media that are widely distributed:
  - (i) Any news, editorial, or advertising statement published in any bona fide newspaper, journal, or magazine, or broadcast over radio or television;
  - (ii) Any gathering or furnishing of information or news by any bona fide reporter, correspondent, or news bureau to news media described in division (A)(7)(b)(i) of this section;
  - (iii) Any publication designed for and distributed to members of any bona fide association or charitable or fraternal non-profit corporation;
  - (iv) Any type of media similar in nature to any item, entity, or activity identified in division (A)(7)(b)(i), (ii), or (iii) of this section.

Ohio Rev. Code Ann. § 1349.19(A)(7). *Encrypted*, *individual*, and *redacted* have the same meanings as in section 1349.19 of the Revised Code. *Id.* § 1354.01(E). *Encryption* “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 Ann. § 1349.19(A)(4). An *individual* means a natural person. *Id.* § 1349.19(A)(5). *Redacted* means “altered or truncated so that no more than the last four digits of a social security number, driver’s license

the protection of both personal information and restricted information<sup>21</sup>) and that reasonably conforms to an “industry recognized cybersecurity framework.”<sup>22</sup> The law further provides that a covered entity’s failure or decision not to comply may not support a private cause of action.<sup>23</sup> The technical requirements for meeting the safe harbor are set forth in greater detail in section 27.04[6][H].<sup>24</sup>

An intermediate appellate court in **Georgia** held, in *McConnell v. Georgia Department of Labor*,<sup>25</sup> that there was no general duty of care to safeguard personal information under Georgia law and none could be inferred from the enactment of Georgia’s security breach notification statute, Ga. Code Ann. §§ 10-1-910 through 10-1-915.

Where claims are brought for failing to comply with state security breach notification laws, they may be based on the timeliness<sup>26</sup> or adequacy of notice.

Where a statute authorizes a private cause of action, a

---

number, state identification card number, account number, or credit or debit card number is accessible as part of the data.” *Id.* § 1349.19(A)(9).

<sup>21</sup>*Restricted information* means “any information about an individual, other than personal information, that, alone or in combination with other information, including personal information, can be used to distinguish or trace the individual’s identity or that is linked or linkable to an individual, if the information is not encrypted, redacted, or altered by any method or technology in such a manner that the information is unreadable, and the breach of which is likely to result in a material risk of identity theft or other fraud to person or property.” Ohio Rev. Code Ann. § 1354.01(E).

*Encrypted*, *individual*, and *redacted* have the same meanings as in section 1349.19 of the Revised Code. *Id.* *Encryption* “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 Ann. § 1349.19(A)(4). An *individual* means a natural person. *Id.* § 1349.19(A)(5). *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.” *Id.* § 1349.19(A)(9).

<sup>22</sup>Ohio Rev. Code Ann. § 1354.02(D).

<sup>23</sup>See Ohio Rev. Code Ann. § 1354.04.

<sup>24</sup>The statutory provisions creating the Ohio safe harbor are reprinted in section 27.09[38]. Guidelines for drafting a written information security program are set forth in section 27.13.

<sup>25</sup>*McConnell v. Georgia Department of Labor*, 345 Ga. App. 669, 678, 814 S.E.2d 790, 798 (2018).

<sup>26</sup>For example, in *In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d 518, 527–28 (N.D. Ill. 2011), a putative class action suit, the court

party may not be able to recover for future, potential harm, if a statute requires a showing of actual harm or injury and there is none at the time of suit.<sup>27</sup> As noted earlier in this subsection, some statutes, such as the one in force in **Alaska**, provide for statutory damages for failing to provide notice of a security breach in accordance with state law.

Even in the absence of an express right to bring a private cause of action, courts applying the law of states or territories that have not expressly excluded private claims for failure to provide adequate notice may allow a claim based on unfair trade practices or potentially even for breach of implied contract.<sup>28</sup>

---

denied defendant's motion to dismiss plaintiffs' claim under the Illinois Personal Information Protection Act (PIPA), 815 Ill. Comp. Stat. Ann. 530/20, for allegedly failing to timely notify affected consumers of a security breach based on skimming credit card information and PIN numbers from PIN pads in defendant's stores. PIPA requires notice "in the most expedient time possible . . . ." 815 Ill. Comp. Stat. Ann. 530/10. In *Michaels*, the defendant alleged that it sent notice within a week of learning of the breach but the court held that plaintiffs' allegation that this time period amounted to an unreasonable delay, was sufficient to defeat defendant's motion to dismiss (which assumes a plaintiff's allegations to be true for purposes of evaluating the motion).

<sup>27</sup>See, e.g., *Pinero v. Jackson Hewitt Tax Service Inc.*, 594 F. Supp. 2d 710, 717 (E.D. La. 2009) (dismissing plaintiff's claim under the Louisiana Database Security Breach Notification Law because, among other things, the court held that a claim could not be maintained based on speculative, future harm); *Ponder v. Pfizer, Inc.*, 522 F. Supp. 2d 793, 797–98 (M.D. La. 2007) (dismissing a putative class action suit alleging that a nine week delay in providing notice that personal information on 17,000 current and former employees had been compromised when an employee installed file sharing software on his company-issued laptop violated Louisiana's Database Security Breach Notification Law because the plaintiff could only allege emotional harm in the form of fear and apprehension of fraud, loss of money and identity theft, but no "actual damage" within the meaning of Louisiana law); see generally *supra* § 27.07 (analyzing the issue of harm in security breach litigation).

<sup>28</sup>See, e.g., *In re TJX Cos. Retail Security Breach Litig.*, 564 F.3d 489 (1st Cir. 2009) (reversing the lower court's dismissal of plaintiffs' unfair trade practices claim under Massachusetts law based on a company's lack of security measures, where the company's conduct allegedly was systematically reckless and aggravated by a failure to give prompt notice when lapses were discovered internally, which allegedly caused widespread and serious harm to other companies and consumers); *In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d 518, 531–32 (N.D. Ill. 2011) (denying defendant's motion to dismiss plaintiffs' claim for breach of an implied contract, holding that plaintiffs had adequately alleged an implicit contractual relationship between plaintiffs and Michaels obligating

**27.08[10][D] Nevada's Statutory Cause of Action Against Data Collectors**

In addition to providing remedies for non-compliance, Nevada also expressly provides a cause of action for data collectors that are required to provide notification. They may bring an action against a person that unlawfully obtained or benefited from personal information obtained from records maintained by the data collector. Under this provision, a prevailing party may recover damages, which may include, without limitation, the reasonable cost of notification (including labor, materials, portage and any other costs reasonably related to providing the notification), reasonable attorneys' fees, and punitive damages.<sup>1</sup> A court may also order a person convicted of unlawfully obtaining or benefiting from personal information to pay restitution to the data collector for the reasonable costs incurred in providing notification (including labor, materials, portage and any other costs reasonably related to providing the notification).<sup>2</sup>

**27.08[10][E] Michigan's Phony Notification Criminal Statute**

**Michigan** criminalizes sending phony security breach notices, which may be sent as part of a phishing scam.<sup>1</sup> Specifically, Michigan provides that any person (or entity) that provides notice of a security breach pursuant to Michigan's security breach statute "when a security breach has not occurred, with the intent to defraud," is guilty of a misdemeanor punishable by imprisonment for not more than thirty days or a fine of not more than \$250 for each violation, or

---

Michaels to take reasonable measures to protect plaintiffs' financial information and notify plaintiffs of a security breach within a reasonable amount of time, in a putative class action suit arising out of a security breach based on skimming credit card information and PIN numbers from PIN pads in defendant's stores).

**[Section 27.08[10][D]]**

<sup>1</sup>See Nev. Rev. Stat. § 603A.900.

<sup>2</sup>See Nev. Rev. Stat. § 603A.910.

**[Section 27.08[10][E]]**

<sup>1</sup>"Phishing is a form of email fraud where senders impersonate legitimate businesses and organizations to try to get recipients to divulge personal information such as passwords and account numbers so the senders can steal the recipient's identity and/or funds from the recipient's account." *Iconix, Inc. v. Tokuda*, 457 F. Supp. 2d 969, 973, 66 Fed. R. Serv. 3d 422 (N.D. Cal. 2006); see generally *infra* § 46.02.

both.<sup>2</sup>

**27.08[10][F] Criminal Sanctions for Willful Disclosures By Government Employees**

**Idaho** makes it misdemeanor subject to a fine of up to \$2,000 and one year in prison for a government employee to intentionally disclose personal information except as permitted by law.<sup>1</sup>

**27.08[10][G] Student Expulsion Based on A Security Breach**

**Texas** law provides that a public school student may be expelled from school for breaching computer security if the conduct involves accessing a computer, computer network or computer system owned by or operated on behalf of a school district and, among other things, “commits a breach of any other computer, computer network or computer system.”<sup>1</sup>

**27.08[11] Contractual Waivers of Notice Obligations**

It is questionable whether any state would enforce a purported waiver of a consumer’s right to notice in the event of a security breach. **Alaska, Arkansas, Colorado, the District of Columbia, Hawaii, Illinois, Kentucky, Maryland, Minnesota, Nebraska, Nevada, North Carolina, Ohio, Utah, Vermont, the U.S. Virgin Islands and Washington**, however, expressly provide that any waiver is contrary to public policy and is void and unenforceable.<sup>1</sup> In addition, **New Hampshire** provides that any attempted waiver

---

<sup>2</sup>Mich. Comp. Laws Ann. § 445.72(12).

**[Section 27.08[10][F]]**

<sup>1</sup>Idaho Code Ann. § 28-51-105.

**[Section 27.08[10][G]]**

<sup>1</sup>Tex. Education Code § 37.007(b)(5).

**[Section 27.08[11]]**

<sup>1</sup>See Alaska Stat. § 45.48.060 (“A waiver of AS 45.48.010—45.48.090 is void and unenforceable.”); Ark. Code Ann. § 4-110-107; Colo. Rev. Stat. Ann. § 6-1-716(2)(e) (“A waiver of these notification rights or responsibilities is void as against public policy.”); D.C. Code § 28-3852(f) (no reference to public policy; just “void and enforceable”); Haw. Rev. Stat. Ann. § 487N-2(h); 815 Ill. Comp. Stat. Ann. 530/10/15; Ky. Rev. Stat. Ann. § 61.933(4); Md. Code Ann., Com. Law § 14-3504(j); Md. Code Ann., State Gov’t § 10-1305(i); Minn. Stat. Ann. § 325E.61(1)(e); Neb. Rev. Stat. § 87-805; Nev. Rev. Stat. Ann. § 603A.100(3); Nev. Rev. Stat. § 603A.100; N.C. Gen. Stat.

of the monetary remedies available when a company fails to provide breach notification shall be void and unenforceable.<sup>2</sup>

### **27.08[12] Data Destruction and Security Freeze Laws**

Some state security breach notification statutes address related security issues such as data destruction,<sup>1</sup> to minimize the risk of identity theft in the event of a security breach (which is also referred to as data minimization), and security freezes,<sup>2</sup> to limit damage in the event of a breach. Other states have enacted similar provisions (but not as part of their security breach notification statutes). Data minimization or destruction statutes are analyzed in section 27.04[6][D] and are reprinted below in section 27.09. They are also discussed briefly in the context of identity theft in chapter 46, may be found in section 46.09. Statutes that require that notice of a consumer's right to obtain a security freeze be included in a security breach notice are addressed in section 27.08[6].

---

§ 75-65(g); Ohio Rev. Code Ann. § 1347.19(H); Utah Code Ann. § 13-44-202(6); Vt. Stat. Ann. tit. 9, § 2435(e); V.I. Code Ann. tit. 14, § 2210; Wash. Code Ann. §§ 19.255.010(12) (persons and businesses), 42.56.590(11) (state agencies).

<sup>2</sup>See N.H. Rev. Stat. Ann. § 359-C:21(I).

#### **[Section 27.08[12]]**

<sup>1</sup>Arizona, Arkansas, California, Colorado, Florida, Georgia, Hawaii, Illinois, Indiana, Kansas, Maryland, Michigan, Minnesota, Montana, Nevada, New Jersey, New Mexico, North Carolina, Oregon, Rhode Island (with respect to driver's records), Tennessee, Texas and Utah have adopted statutes requiring that records containing personal information be destroyed, rather than retained, when no longer needed. *See supra* § 27.04[6][D]. New York, by regulation, has imposed this requirement as well on covered entities in the financial services industry. *See supra* § 27.04[6][K].

<sup>2</sup>These states include Alaska, Colorado, Delaware, the District of Columbia, Georgia, Hawaii, Idaho, Illinois, Kansas, Louisiana, Maine, Minnesota, Massachusetts, Montana, New Hampshire, New Jersey, North Carolina, Oklahoma, South Dakota, Tennessee, Vermont, Washington, West Virginia, Wisconsin and Wyoming. *See infra* § 46.09[1]. Connecticut and Delaware require that notice of a consumer's ability to place a credit freeze on their credit file be provided. *See* Conn. Gen. Stat. Ann. § 36a-701b(b)(2)(B); Del. Code Ann. tit. 6, § 12B-102(e); *see generally supra* § 27.08[9]. Since September 2018, there is no charge to consumers in any state for placing a credit freeze on a consumer's account and obtaining yearlong fraud alerts.

**27.08[13] Compliance Checklist**

In evaluating whether and how the owner or licensee of data must provide notice to consumers in the event of a security breach,<sup>1</sup> the following checklist may be helpful:

**Is Notice Required?**

- Was a security breach experienced by a government agency, business or private person?<sup>2</sup>
- Is notice required based on the laws of those states where affected consumers reside (and if so to whom—data owners, consumers, state regulators and/or credit bureaus)?
- Is notice alternatively required to residents of particular states based on the laws of the jurisdiction(s) where the company conducts business?<sup>3</sup>
- If a business determines that a breach has or may have occurred, it is required to undertake the specific investigatory steps set forth under Alabama law for covered entities, with respect to sensitive personally identifying information, as set forth in that law, which requires a covered entity to “conduct a good faith and prompt investigation” that includes all of the following:
  - (1) An assessment of the nature and scope of the breach.
  - (2) Identification of any sensitive personally identifying information that may have been involved in the breach and the identity of

---

**[Section 27.08[13]]**

<sup>1</sup>Assuming an obligation to provide notice exists, persons or entities that manage data on behalf of others are required in all states (except Wyoming) to notify the owner or licensee of a breach, who in turn is required to provide notice to consumers. In Wyoming, notice to consumers must be sent by the party that has agreed contractually to provide notice or, in the absence of an agreement, the person who has the most direct business relationship with affected state residents. *See* Wyo. Stat. Ann. § 40-12-502(g).

<sup>2</sup>Some state laws apply to all three, while some do not. A number of states use specific terms for the type of businesses that may be required to provide notice, such as a *covered entity* (under Alabama, Colorado and Florida law).

<sup>3</sup>For example, statutes such as those in effect in Texas or Wisconsin may require that notice be provided to residents of other states (beyond what would be required based on the residence of affected consumers). *See supra* § 27.08[1] (discussing this issue).

any individuals to whom that information relates.

- (3) A determination of whether the sensitive personally identifying information has been acquired or is reasonably believed to have been acquired by an unauthorized person,<sup>4</sup> and is reasonably likely to cause substantial harm to the individuals to whom the information relates.
- (4) Identification and implementation of measures to restore the security and confidentiality of the systems compromised in the breach.<sup>5</sup>
- Was the security of unencrypted<sup>6</sup> personal information within the scope of applicable statutes that cover information that was stored electronically (or potentially in any form, depending on the applicability of Arkansas, Indiana, Hawaii, Massachusetts, North Carolina and Washington law and the nature of the information) compromised?
  - Was encryption used and if so was it at least 128-bit encryption or consistent with industry best practices?<sup>7</sup>
  - ◻ Does disclosure compromise the security, confidentiality or integrity of the data?
  - ◻ Was the disclosure made to an employee or

---

<sup>4</sup>To make this determination, the statute further requires a covered entity to consider:

- (1) Indications that the information is in the physical possession and control of a person without valid authorization, such as a lost or stolen computer or other device containing information.
- (2) Indications that the information has been downloaded or copied.
- (3) Indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.
- (4) Whether the information has been made public.

Ala. Code § 8-38-4(b).

<sup>5</sup>Ala. Code § 8-38-4(a); *see generally supra* § 27.08[4].

<sup>6</sup>Notice may be required under various state laws even where personal information was encrypted if the information was or may have been acquired by an unauthorized person or if the means to decrypt it was obtained or if the loss is reasonably believed to allow access to the information (for example, if weak encryption was used) or if it could lead to identity theft or fraud.

<sup>7</sup>*See supra* § 27.08[3][C].

agent acting in good faith and for business purposes (and not used or subject to further disclosure)?

- Was the data that was exposed part of a multi-person database?<sup>8</sup>
- ☐ Was the disclosure made pursuant to a search warrant, subpoena or court order?
- ☐ Was the compromised information defined as *personal information* or otherwise covered by applicable statutes? Was a person's name<sup>9</sup> (or any information concerning a natural person which, because of the name, personal mark, or other identifier, can be used to identify the person)<sup>10</sup> disclosed in combination with<sup>11</sup> his or her:
  - Social Security number<sup>12</sup>
  - driver's license or state identification card<sup>13</sup> or voter ID card or other official identification,<sup>14</sup> passport number or other U.S.-issued identification number<sup>15</sup> or military ID<sup>16</sup> or identification number issued on a government document that is

---

<sup>8</sup>Notification is only required in some states where compromised data was stored in a multi-person database. *See supra* § 27.08[3][A].

<sup>9</sup>Most statutes focus on an individual's first name or initial and last name. Prior to 2014, Florida also included a middle name and last name.

<sup>10</sup>This broader definition is used under New York law.

<sup>11</sup>States increasingly are focusing on account credentials. Hence, even if a person's name is not disclosed in combination with other data elements but a user ID and password or other account credentials were exposed, there may be an obligation to provide notice under some state laws (or more generally to avoid liability in litigation for failing to provide, or failing to timely provide, notice of a breach; *supra* § 27.07).

<sup>12</sup>Disclosure of merely the last four or five digits would not require notification in all states.

<sup>13</sup>Disclosure of merely the last four or five digits would not require notification in all states.

<sup>14</sup>These elements are listed in Puerto Rico's statute.

<sup>15</sup>Oregon's notification statute includes these elements. Passport numbers are also included in the security breach notification laws in effect in Connecticut, Delaware, Florida, Maryland, Michigan and North Carolina. Other state laws apply to employer IDs, which presumably would include military IDs.

<sup>16</sup>Florida and Colorado include both a passport, like Connecticut, Michigan, North Carolina, and Oregon, and military ID. Other state secu-

- used to verify the identity of a specific individual.<sup>17</sup>
- account number, debit card or credit card number (or unique electronic identification numbers or routing codes)<sup>18</sup>
  - security or access code or password that would permit access to an account
  - biometric data, such as a fingerprint, voice print, or retina or iris image or other unique physical representation<sup>19</sup>
  - deoxyribonucleic acid profile<sup>20</sup>
  - date of birth, mother's maiden name, identification number assigned by an employer or digitized or electronic signature<sup>21</sup>
  - "information or data collected through the use or operation of an automated license plate recognition system"<sup>22</sup>
  - Individual Taxpayer ID number<sup>23</sup>
  - tax information and work-related evaluations,<sup>24</sup>
  - an identity protection personal identification number issued by the IRS,<sup>25</sup> and/or

rity breach notification laws (including Connecticut, Florida, Michigan, North Carolina and North Dakota) apply to employer IDs, which presumably would include military IDs. Still others, such as Oregon, apply to IDs issued by the United States, which also presumably would include military IDs.

<sup>17</sup>Alabama includes this data element in its security breach notification statute.

<sup>18</sup>This broader language is used under Nebraska law.

<sup>19</sup>At least ten states require notification of security breaches involving biometric data. *See supra* § 27.08[3][B].

<sup>20</sup>This element is included in Wisconsin law.

<sup>21</sup>North Dakota's security breach notification statute includes these elements.

<sup>22</sup>License plate information was added to California's security breach notification law effective January 1, 2016.

<sup>23</sup>This element is included in the security breach notification statutes in effect in Connecticut, Delaware, Florida, Maryland, Michigan, Montana, North Carolina and Wyoming.

<sup>24</sup>These elements are included in Puerto Rico's statute.

<sup>25</sup>This information is included in Montana's statute.

- medical information or health insurance information.<sup>26</sup> and/or
- Did the breach expose: (i) the full, unencrypted magnetic strip of a credit card or debit card, (ii) the full, unencrypted account information contained in an identification device, or (iii) the unencrypted primary account number on a credit card or debit card or identification device, plus any of the following if not encrypted: cardholder's name, expiration date or service code?<sup>27</sup>
- Even if these data elements were not exposed, was a person's name and email address, without more, exposed, such that notification might be required if the data could provide access to a financial account or resources?<sup>28</sup>
- Was the information—although unencrypted—redacted or otherwise obscured such that notice may not be required under all statutes?
- Is the disclosure unlikely to lead to identity theft or criminal activity (or create “no reasonable likelihood of financial harm” to affected consumers under Iowa's statute or “reasonably likely to cause substantial harm to whom the information relates” under Alabama law and (with minor modification) Florida law), such that exceptions to notification obligations recognized in some states may apply? Conversely, are there any indications (within the meaning of New York law) that the information has been acquired by an un-

---

<sup>26</sup>This information is included in the California, Florida, Illinois, Maryland, Missouri, North Dakota, Rhode Island and Wyoming statutes. Medical information may also trigger notification obligations under the notification laws in effect in Arkansas, Oregon, Montana and Puerto Rico. Nevada includes a variation in its security breach notification law, a “medical identification number or a health insurance identification number . . . .”

<sup>27</sup>See *infra* § 27.08[14] (additional rules for credit and debit card data).

<sup>28</sup>Disclosure in this circumstance is required in North Carolina. See N.C. Gen. Stat. Ann. §§ 14-113.20(b)(8), 75-61(10), 75-65(a).

authorized person, downloaded or copied or used?

- Was the information that was compromised otherwise publicly available?<sup>29</sup>
- ☐ Did the breach result from the theft of a laptop protected by encryption? Was the laptop password protected?<sup>30</sup>
- ☐ Was the material in paper or other non-electronic form, such that most (but not all) notification statutes will be inapplicable?
- ☐ Was the personal information subject to a breach “used in the course of the person’s business, vocation, occupation, or volunteer activities . . . .”? If not, notification may not be required under Iowa and Oregon law.
- ☐ Did the breach involve criminal intelligence systems such that notification would not be required under Virginia law?<sup>31</sup>
- If notice to consumers is not required, has the basis for this conclusion been documented and retained for three years in Maryland and South Dakota or five years in Alabama, Alaska, Florida, Iowa, Louisiana, Missouri, New Jersey and Oregon?
- If notice to consumers is not required, must notice of that fact (and potentially documentation) be provided to state officials in Alaska, Florida, South Dakota or Vermont (or, upon the request of the Attorney General, within 30 days for residents of Louisiana)?<sup>32</sup>

If Notice to Consumers is Required, Must Notices to State Agencies and/or Credit Reporting Agencies Be Filed (and, if so, When)?<sup>33</sup>

- Is there an obligation to notify credit reporting agencies? If so, is such notice required in advance of consumer notification and what must it contain?<sup>34</sup>
- Is there an obligation to notify the State Attorney

---

<sup>29</sup>See *supra* § 27.08[3][F].

<sup>30</sup>See *supra* § 27.08[3][D].

<sup>31</sup>See *supra* § 27.08[3][G].

<sup>32</sup>See *supra* § 27.08[8].

<sup>33</sup>See *supra* § 27.08[8].

<sup>34</sup>See *supra* § 27.08[7]. Minnesota, for example, requires that such notice be provided within 48 hours of discovering circumstances that would

General (and if so, before, at the same time as or after notice will be sent to consumers)?<sup>35</sup>

- Must (or should) a police report be filed? A number of states require permission of law enforcement agents before a notice may be sent, which presupposes that a report has been filed.<sup>36</sup>
- If notice need not be sent to consumers, notice of this determination may need to be sent to the Attorney General's office in Alaska and Vermont and the Department of Legal Affairs in Florida. Note that these filings may or may not be kept confidential.<sup>37</sup>

#### Timing of Consumer Notice and Potential Delays

- If there is an obligation to notify consumers, must state police be notified in advance of any consumer disclosure?
- How quickly must notice to consumers be sent under applicable laws? While the language varies, all statutes require an expeditious response, subject to some exceptions for police investigations or to restore the integrity of a network. Ohio and, subject to potential extensions, Rhode Island, Tennessee, Vermont, Washington and Wisconsin require that, at the latest, notice must be sent within forty-five (45) days following notice or discovery of a breach, Connecticut generally requires notice within ninety (90) days and, subject to a potential fifteen day extension and some exceptions, Florida requires notice within thirty (30) days.
- May notice be delayed to allow for an evaluation of whether personal information in fact has been compromised or to detect and correct the security problem?
- Is delay permitted to obtain sufficient contact information?
- Is a delay required based on a request from law enforcement personnel (to make sure the notice

---

require notice to be provided to more than 500 people.

<sup>35</sup>See *supra* § 27.08[8].

<sup>36</sup>See *supra* § 27.08.

<sup>37</sup>See *supra* § 27.08[8]

does not compromise an ongoing criminal investigation)?<sup>38</sup>

#### Method of Notice

- What form of notice (i.e., mail, electronic, fax, phone) may be provided in the applicable jurisdictions?<sup>39</sup>
  - Notice by mail is permissible in all states in all cases. Other forms of notice may be permitted depending on the states involved and the facts of a given security breach.
  - May notice be provided pursuant to an information security policy?
  - Is substitute notice permissible or desirable?
  - Can uniform notice be provided or is it necessary (or if permissible, nonetheless more economical or desirable) to use different forms of notice for residents of different states?<sup>40</sup>
    - Note that Massachusetts prohibits a description of the nature of the breach to be disclosed to Massachusetts residents, while other states require this very disclosure
    - Note that Maryland and Massachusetts require state-specific information to be included in any notice to state residents
  - Is email notice permitted or desirable?<sup>41</sup> Email may be inexpensive and provide quick notice, but may generate more adverse publicity than notice sent by U.S. mail, is not permitted in all cases in all states, and does not allow for message forwarding if an address is no longer valid or is not checked by its owner.
    - Does the company hope to send a single communication to residents of all affected states or is it willing to use differ-

<sup>38</sup>As a practical matter, state laws conflict on this point. *See supra* §§ 27.08[1], 27.08[4].

<sup>39</sup>*See supra* § 17.08[5].

<sup>40</sup>*See supra* § 27.08[6].

<sup>41</sup>*See supra* § 27.08[5].

ent means of notifying residents of particular states?

- Are there record keeping requirements associated with the chosen forms of notice?

Text of the Notice and Additional Requirements

- Do the communications to consumers incorporate the specific style mandated and/or text required for security breach notices sent to residents of California, Hawaii, Iowa, Maryland, Massachusetts, Michigan, Missouri, New Hampshire, New York, North Carolina, Oregon, Rhode Island, Vermont, Washington, West Virginia, Wisconsin and Wyoming<sup>42</sup> (or the notice about identity theft mitigation and/or prevention services required for residents of Connecticut and Delaware)?
- Is the notice clear, written in plain language, and conspicuous?<sup>43</sup>
- Is there an obligation to provide a hotline for affected consumers from Hawaii, North Carolina and Vermont to obtain additional information and assistance?<sup>44</sup>
- Is there an obligation to provide notice about identity theft prevention and/or mitigation services or credit monitoring or a consumer's ability to place a credit freeze on his or her credit file?<sup>45</sup>
- Have recordkeeping requirements (including compliance with retention obligations) been met for notice by phone or where notice is not required?<sup>46</sup>

**27.08[14] Additional Rules for Credit and Debit Card Account Information**

**Nevada** and **Washington** compel compliance with the Payment Card Industry (PCI) Data Security Standards and provide limited safe harbors when security breaches occur notwithstanding PCI compliance. Washington's law, which is the broader of the two, provides that processors, businesses and vendors may be liable to financial institutions for

<sup>42</sup>See *supra* § 27.08[6].

<sup>43</sup>See *supra* § 27.08[6].

<sup>44</sup>Vermont requires that the telephone number provided be toll-free, if available. Vt. Stat. Ann. tit. 9, § 2435(b)(5)(D).

<sup>45</sup>See *supra* § 27.08[9].

<sup>46</sup>See *supra* § 27.08[3][A].

any breach of the security of (i) the full, unencrypted magnetic strip of a credit card or debit card, (ii) the full, unencrypted account information contained in an identification device, or (iii) the unencrypted primary account number on a credit card or debit card or identification device, plus any of the following if not encrypted: cardholder's name, expiration date or service code.<sup>1</sup> Liability may be imposed where a processor or business fails to take reasonable care to guard against unauthorized access to account information in its possession and the failure is found to be the proximate cause of the breach.<sup>2</sup> The statute, however, provides an exemption from liability for any security breach where (a) account information was encrypted at the time of the breach or (b) the processor, business or vendor was certified in compliance with the data security standards adopted by the payment card industry (PCI) council.<sup>3</sup> A processor, business or vendor will be considered compliant if its PCI compliance was validated by an annual security assessment that occurred no longer than one year prior to a breach.<sup>4</sup> The remedies provided by the Washington statute are cumulative, although it authorizes the trier of fact to reduce damages awarded to a financial institution by any amount that it recovered from a credit card company in connection with the breach.<sup>5</sup>

The Nevada statute requires any data collector doing business in the state that accepts a payment card in connection with the sale of goods or services to comply with the PCI Data Security Standard (DSS).<sup>6</sup> Data controllers not required to comply with PCI DSS under the statute are required to encrypt personal information when moved or transferred.<sup>7</sup> Where these requirements are met (or an exemption applies),<sup>8</sup> the statute provides that a data controller may not be held liable for damages for breach of the security of its data

---

[Section 27.08[14]]

<sup>1</sup>See Wash. Code Ann. § 19.255.020(1)(a).

<sup>2</sup>See Wash. Code Ann. § 19.255.020(3)(a).

<sup>3</sup>See Wash. Code Ann. § 19.255.020(2).

<sup>4</sup>See Wash. Code Ann. § 19.255.020(2).

<sup>5</sup>See Wash. Code Ann. § 19.255.020(7).

<sup>6</sup>Nev. Rev. Stat. Ann. § 603A.215(1).

<sup>7</sup>Nev. Rev. Stat. Ann. § 603A.215(2).

<sup>8</sup>See Nev. Rev. Stat. Ann. § 603A.215(4).

INFORMATION, NETWORK AND DATA SECURITY

system, provided the breach is not caused by the gross negligence or intentional misconduct of the data collector, its officers, employees or agents.<sup>9</sup>

Copies of the Nevada and Washington statutes are reprinted below in section 27.09.

PCI security guidelines are analyzed in greater detail in section 27.05.

---

<sup>9</sup>Nev. Rev. Stat. Ann. § 603A.215(3).

# E-COMMERCE & INTERNET LAW: TREATISE WITH FORMS 2D 2019

*Ian C. Ballon*

**NEW AND  
IMPORTANT  
FEATURES  
FOR 2019  
NOT FOUND  
ELSEWHERE**

**THE PREEMINENT  
INTERNET AND  
MOBILE LAW  
TREATISE FROM A  
LEADING INTERNET  
LITIGATOR — NOW A  
5 VOLUME SET!**



To order call **1-888-728-7677**  
or visit **[legalsolutions.thomsonreuters.com](http://legalsolutions.thomsonreuters.com)**

## Key Features of E-Commerce & Internet Law

- ◆ The California Consumer Privacy Act, GDPR, California IoT security statute, Vermont data broker registration law, Ohio safe harbor statute and other important privacy and cybersecurity laws
- ◆ Understanding conflicting law on mobile contract formation, unconscionability and enforcement of arbitration and class action waiver clauses
- ◆ The most comprehensive analysis of the TCPA's application to text messaging and its impact on litigation found anywhere
- ◆ Complete analysis of the Cybersecurity Information Sharing Act (CISA), state security breach statutes and regulations, and Defend Trade Secrets Act (DTSA) and their impact on screen scraping and database protection, cybersecurity information sharing and trade secret protection, privacy obligations and the impact that Terms of Use and other internet and mobile contracts may have in limiting the broad exemption from liability otherwise available under CISA
- ◆ Comprehensive and comparative analysis of the platform liability of Internet, mobile and cloud site owners, and service providers, for user content and misconduct under state and federal law
- ◆ Understanding the laws governing SEO and SEM and their impact on e-commerce vendors, including major developments involving internet advertising and embedded and sponsored links
- ◆ AI, screen scraping and database protection
- ◆ Strategies for defending cybersecurity breach and data privacy class action suits
- ◆ Copyright and Lanham Act fair use, patentable subject matter, combating genericide, right of publicity laws governing the use of a person's images and attributes, initial interest confusion, software copyrightability, damages in internet and mobile cases, the use of icons in mobile marketing, new rules governing fee awards, and the applicability and scope of federal and state safe harbors and exemptions
- ◆ How to enforce judgments against foreign domain name registrants
- ◆ Valuing domain name registrations from sales data
- ◆ Compelling the disclosure of the identity of anonymous and pseudonymous tortfeasors and infringers
- ◆ Exhaustive statutory and case law analysis of the Digital Millennium Copyright Act, the Communications Decency Act (including exclusions created by FOSTA-SESTA), the Video Privacy Protection Act, and Illinois Biometric Privacy Act
- ◆ Analysis of the CLOUD Act, BOTS Act, SPEECH Act, Consumer Review Fairness Act, N.J. Truth-in-Consumer Contract, Warranty and Notice Act, Family Movie Act and more
- ◆ Practical tips, checklists and forms that go beyond the typical legal treatise
- ◆ Clear, concise, and practical analysis

## AN ESSENTIAL RESOURCE FOR ANY INTERNET AND MOBILE, INTELLECTUAL PROPERTY OR DATA PRIVACY/ CYBERSECURITY PRACTICE

*E-Commerce & Internet Law* is a comprehensive, authoritative work covering law, legal analysis, regulatory issues, emerging trends, and practical strategies. It includes practice tips and forms, nearly 10,000 detailed footnotes, and references to hundreds of unpublished court decisions, many of which are not available elsewhere. Its unique organization facilitates finding quick answers to your questions.

The updated new edition offers an unparalleled reference and practical resource. Organized into five sectioned volumes, the 59 chapters cover:

- Sources of Internet Law and Practice
- Intellectual Property
- Licenses and Contracts
- Data Privacy, Cybersecurity and Advertising
- The Conduct and Regulation of E-Commerce
- Internet Speech, Defamation, Online Torts and the Good Samaritan Exemption
- Obscenity, Pornography, Adult Entertainment and the Protection of Children
- Theft of Digital Information and Related Internet Crimes
- Platform liability for Internet Sites and Services (Including Social Networks, Blogs and Cloud services)
- Civil Jurisdiction and Litigation

### Distinguishing Features

- ◆ Clear, well written and with a practical perspective based on how issues actually play out in court (not available anywhere else)
- ◆ Exhaustive analysis of circuit splits and changes in the law combined with a common sense, practical approach for resolving legal issues, doing deals, documenting transactions and litigating and winning disputes
- ◆ Covers laws specific to the Internet and explains how the laws of the physical world apply to internet and mobile transactions and liability risks
- ◆ Addresses both law and best practices
- ◆ Comprehensive treatment of intellectual property, data privacy and mobile and Internet security breach law

---

**Volume 1**


---

**Part I. Sources of Internet Law and Practice: A Framework for Developing New Law**

- Chapter* 1. Context for Developing the Law of the Internet  
 2. A Framework for Developing New Law  
 3. [Reserved]

**Part II. Intellectual Property**

4. Copyright Protection in Cyberspace  
 5. Database Protection, Screen Scraping and the Use of Bots and Artificial Intelligence to Gather Content and Information  
 6. Trademark, Service Mark, Trade Name and Trade Dress Protection in Cyberspace  
 7. Rights in Internet Domain Names

---

**Volume 2**


---

- Chapter* 8. Internet Patents  
 9. Unique Intellectual Property Issues in Search Engine Marketing, Optimization and Related Indexing, Information Location Tools and Internet and Social Media Advertising Practices  
 10. Misappropriation of Trade Secrets in Cyberspace  
 11. Employer Rights in the Creation and Protection of Internet-Related Intellectual Property  
 12. Privacy and Publicity Rights of Celebrities and Others in Cyberspace  
 13. Idea Protection and Misappropriation

**Part III. Licenses and Contracts**

14. Documenting Internet Transactions: Introduction to Drafting License Agreements and Contracts  
 15. Drafting Agreements in Light of Model and Uniform Contract Laws: UCITA, the UETA, Federal Legislation and the EU Distance Sales Directive  
 16. Internet Licenses: Rights Subject to License and Limitations Imposed on Content, Access and Development  
 17. Licensing Pre-Existing Content for Use Online: Music, Literary Works, Video, Software and User Generated Content Licensing Pre-Existing Content  
 18. Drafting Internet Content and Development Licenses  
 19. Website Development and Hosting Agreements  
 20. Website Cross-Promotion and Cooperation: Co-Branding, Widget and Linking Agreements  
 21. Obtaining Assent in Cyberspace: Contract Formation for Click-Through and Other Unilateral Contracts  
 22. Structuring and Drafting Website Terms and Conditions  
 23. ISP Service Agreements

---

**Volume 3**


---

- Chapter* 24. Software as a Service: On-Demand, Rental and Application Service Provider Agreements

**Part IV. Privacy, Security and Internet Advertising**

25. Introduction to Consumer Protection in Cyberspace  
 26. Data Privacy  
 27. Cybersecurity: Information, Network and Data Security  
 28. Advertising in Cyberspace

---

**Volume 4**


---

- Chapter* 29. Email and Text Marketing, Spam and the Law of Unsolicited Commercial Email and Text Messaging

30. Online Gambling

**Part V. The Conduct and Regulation of Internet Commerce**

31. Online Financial Transactions and Payment Mechanisms  
 32. Online Securities Law  
 33. Taxation of Electronic Commerce  
 34. Antitrust Restrictions on Technology Companies and Electronic Commerce  
 35. State and Local Regulation of the Internet  
 36. Best Practices for U.S. Companies in Evaluating Global E-Commerce Regulations and Operating Internationally

**Part VI. Internet Speech, Defamation, Online Torts and the Good Samaritan Exemption**

37. Defamation, Torts and the Good Samaritan Exemption (47 U.S.C.A. § 230)  
 38. Tort and Related Liability for Hacking, Cracking, Computer Viruses, Disabling Devices and Other Network Disruptions  
 39. E-Commerce and the Rights of Free Speech, Press and Expression In Cyberspace

**Part VII. Obscenity, Pornography, Adult Entertainment and the Protection of Children**

40. Child Pornography and Obscenity  
 41. Laws Regulating Non-Obscene Adult Content Directed at Children  
 42. U.S. Jurisdiction, Venue and Procedure in Obscenity and Other Internet Crime Cases

**Part VIII. Theft of Digital Information and Related Internet Crimes**

43. Detecting and Retrieving Stolen Corporate Data  
 44. Criminal and Related Civil Remedies for Software and Digital Information Theft  
 45. Crimes Directed at Computer Networks and Users: Viruses and Malicious Code, Service Disabling Attacks and Threats Transmitted by Email

---

**Volume 5**


---

- Chapter* 46. Identity Theft

47. Civil Remedies for Unlawful Seizures

**Part IX. Liability of Internet Sites and Service (Including Social Networks and Blogs)**

48. Assessing and Limiting Liability Through Policies, Procedures and Website Audits  
 49. The Liability of Platforms (including Website Owners, App Providers, eCommerce Vendors, Cloud Storage and Other Internet and Mobile Service Providers) for User Generated Content and Misconduct  
 50. Cloud, Mobile and Internet Service Provider Liability and Compliance with Subpoenas and Court Orders  
 51. Web 2.0 Applications: Social Networks, Blogs, Wiki and UGC Sites

**Part X. Civil Jurisdiction and Litigation**

52. General Overview of Cyberspace Jurisdiction  
 53. Personal Jurisdiction in Cyberspace  
 54. Venue and the Doctrine of Forum Non Conveniens  
 55. Choice of Law in Cyberspace  
 56. Internet ADR  
 57. Internet Litigation Strategy and Practice  
 58. Electronic Business and Social Network Communications in the Workplace, in Litigation and in Corporate and Employer Policies  
 59. Use of Email in Attorney-Client Communications

*“Should be on the desk of every lawyer who deals with cutting edge legal issues involving computers or the Internet.”*

**Jay Monahan**

**General Counsel, ResearchGate**

\*\*\*\*\*

## ABOUT THE AUTHOR

\*\*\*\*\*

### IAN C. BALLON

Ian Ballon is Co-Chair of Greenberg Traurig LLP's Global Intellectual Property and Technology Practice Group and is a litigator based in the firm's Silicon Valley and Los Angeles offices. He defends data privacy, cybersecurity breach, TCPA, and other Internet and mobile class action suits and litigates copyright, trademark, patent, trade secret, right of publicity, database and other intellectual property matters, including disputes involving Internet-related safe harbors and exemptions and platform liability.



Mr. Ballon was the recipient of the 2010 Vanguard Award from the State Bar of California's Intellectual Property Law Section. He also has been recognized by *The Los Angeles and San Francisco Daily Journal* as one of the Top 75 Intellectual Property litigators, Top Cybersecurity and Artificial Intelligence (AI) lawyers, and Top 100 lawyers in California.

In 2017 Mr. Ballon was named a "Groundbreaker" by *The Recorder* at its 2017 Bay Area Litigation Departments of the Year awards ceremony and was selected as an "Intellectual Property Trailblazer" by the *National Law Journal*.

Mr. Ballon was named as the Lawyer of the Year for information technology law in the 2019, 2018, 2016 and 2013 editions of *The Best Lawyers in America* and is listed in Legal 500 U.S., *The Best Lawyers in America* (in the areas of information technology and intellectual property) and Chambers and Partners USA Guide in the areas of privacy and data security and information technology. He also serves as Executive Director of Stanford University Law School's Center for E-Commerce in Palo Alto.

Mr. Ballon received his B.A. *magna cum laude* from Tufts University, his J.D. *with honors* from George Washington University Law School and an LLM in international and comparative law from Georgetown University Law Center. He also holds the C.I.P.P./U.S. certification from the International Association of Privacy Professionals (IAPP).

In addition to *E-Commerce and Internet Law: Treatise with Forms 2d edition*, Mr. Ballon is the author of *The Complete CAN-SPAM Act Handbook* (West 2008) and *The Complete State Security Breach Notification Compliance Handbook* (West 2009), published by Thomson West ([www.IanBallon.net](http://www.IanBallon.net)).

He may be contacted at [BALLON@GTLAW.COM](mailto:BALLON@GTLAW.COM) and followed on Twitter and LinkedIn (@IanBallon).

**Contributing authors:** Parry Aftab, Ed Chansky, Francoise Gilbert, Tucker McCrady, Josh Raskin, Tom Smedinghoff and Emilio Varanini.

## NEW AND IMPORTANT FEATURES FOR 2019

- > A comprehensive analysis of the **California Consumer Information Privacy Act**, **California's Internet of Things (IoT) security statute**, **Vermont's data broker registration law**, **Ohio's safe harbor** for companies with written information security programs, and other new state laws governing cybersecurity (chapter 27) and data privacy (chapter 26)
- > An exhaustive analysis of **FOSTA-SESTA** and what companies should do to maximize CDA protection in light of these new laws (chapter 37)
- > The **CLOUD Act** (chapter 50)
- > Understanding **the TCPA after ACA Int'l** and significant new cases & circuit splits (chapter 29)
- > Fully updated **50-state compendium** of security breach notification laws, with a **strategic approach** to handling notice to consumers and state agencies (chapter 27)
- > **Platform liability and statutory exemptions and immunities** (including a comparison of "but for" liability under the CDA and DMCA, and the latest law on secondary trademark and patent liability) (chapter 49)
- > Applying **the single publication rule** to websites, links and uses on social media (chapter 37)
- > The complex array of potential liability risks from, and remedies for, **screen scraping, database protection and use of AI to gather data and information online** (chapter 5)
- > State online dating and revenge porn laws (chapter 51)
- > **Circuit splits on Article III standing in cybersecurity litigation** (chapter 27)
- > Revisiting **sponsored link, SEO and SEM practices and liability** (chapter 9)
- > **Website and mobile accessibility** (chapter 48)
- > **The Music Modernization Act's impact on copyright preemption and DMCA protection for pre-1972 musical works** (chapter 4)
- > **Compelling the disclosure of passwords and biometric information to unlock a mobile phone, tablet or storage device** (chapter 50)
- > Cutting through the jargon to make sense of **clickwrap, browsewrap, scrollwrap and sign-in wrap agreements (and what many courts and lawyers get wrong about online contract formation)** (chapter 21)
- > The latest case law, trends and strategy for **defending cybersecurity and data privacy class action suits** (chapters 25, 26, 27)
- > **Click fraud** (chapter 28)
- > Updated **Defend Trade Secrets Act** and **UTSA** case law (chapter 10)
- > **Drafting enforceable arbitration clauses and class action waivers** (with new sample provisions) (chapter 22)
- > **Applying the First Sale Doctrine to the sale of digital goods and information** (chapter 16)
- > **The GDPR, ePrivacy Directive and transferring data from the EU/EEA** (by Francoise Gilbert) (chapter 26)
- > **Patent law** (updated by Josh Raskin) (chapter 8)
- > **Music licensing** (updated by Tucker McCrady) (chapter 17)
- > **Mobile, Internet and Social Media contests & promotions** (updated by Ed Chansky) (chapter 28)
- > **Conducting a risk assessment and creating a Written Information Security Assessment Plan (WISP)** (by Thomas J. Smedinghoff) (chapter 27)

**SAVE 20% NOW!!**

To order call **1-888-728-7677**  
or visit **[legalsolutions.thomsonreuters.com](http://legalsolutions.thomsonreuters.com)**,  
enter promo code **WPD20** at checkout

List Price: \$2,567.50  
Discounted Price: \$2,054