Bloomberg Law

Privacy and Security Law Report®

Data Breach Notification

Six states amended their data breach notification laws in 2016, adding a few more squares to the patchwork of state laws, and serving as a good reminder that, while there are broad, overarching consistencies among the state statutes, there are nuances that can dramatically alter an entity's notification obligations depending on the particular facts of the incident and which states' laws may be impacted, the authors write.

Cyber Alert—Breach Roundup, Part I: U.S. State Data Breach Notification Laws Highlights and Trends

BY KIM PERETTI

In many respects, 2016 was a remarkable year, but one constant with recent history is that multiple states (six in 2016) amended their breach notification statutes. As is commonly stated, the U.S. operates under a patchwork of breach notification statutes implemented at the state level, and each year several states amend their laws to either bring them in line with other states, jump on developing trends or enact more stringent requirements that could eventually become widely adopted. 2016 was no exception.

As a general overview, the states' breach notification statutes generally trigger notification obligations when a ''breach'' impacts ''personal information,'' as those terms are defined by each state statute. Most often, personal information is defined as an individual's name (more specifically the first name or first initial and last name) in combination with a secondary data element such as a Social Security number or driver's license number. A breach is often defined, in essence, as the unauthorized acquisition of personal information. When notice obligations trigger, entities must notify all impacted state residents of the incident. Many state laws also require that entities notify state regulators, such as state attorneys general, of the data breach. Notice is often sent to individuals in writing through postal mail, but in some cases can be sent via email or through posting a notification on a company's website and notifying statewide media.

Kim Peretti is a partner a Alston & Bird's Washington office and is co-chair of the firm's Cybersecurity Preparedness & Response Team.

Statutory Updates

California—Effective Jan. 1, 2017 (Cal. Civ. Code § § 1798.29, 1798.82).

Limiting the encryption safe harbor. California was one of several states to limit its ''safe harbor'' protections for breach notifications when encrypted data is compromised. Many states only require notification when compromised data is unencrypted, meaning that entities do not need to notify individuals of incidents where encrypted data is compromised. This creates a potential loophole under a technical reading of such statutes where notice is not required if the compromised data was encrypted, even if the data was still at risk because the encryption key or password encrypting

the data was also compromised. Previously, California required notice to impacted individuals when ''unencrypted personal information'' was acquired by an unauthorized person. The updated statute will now also require notice when ''encrypted personal information'' is acquired ''and the encryption key or security credential'' was also acquired and the entity has a ''reasonable belief that the encryption key or security credential could render that personal information readable or [usable].''

Formatting requirements. California also made an important change to its statute that became effective on Jan. 1, 2016, by becoming the first (and still only) state to mandate formatting requirements for individual notification letters. Under the California statute, notice letters to individuals must be titled ''Notice of Data Breach'' and must include the following headings: ''What Happened,'' ''What Information Was Involved,'' ''What We Are Doing,'' ''What You Can Do'' and ''For More Information.'' California also provides a ''model security breach notification form'' showcasing these formatting requirements.

Illinois—Effective Jan. 1, 2017 (815 ILCS § § 530/5, 530/10, 530/45, 530/50)

Limiting the encryption safe harbor. Similar to California, Illinois updated its law to require notification when encrypted data is compromised along with the ''keys to unencrypt or unredact or otherwise read the name or data elements that have been acquired.''

Required implementation of ''reasonable security measures.'' Illinois now requires that any entity that owns, licenses or maintains ''personal information concerning an Illinois resident'' must ''implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure.'' The statute now requires that when entities enter into contracts to disclose personal information to other entities, the contract must require that the person to whom the information is disclosed agrees to implement reasonable security measures.

Username + password incidents trigger limited notice obligations. Illinois joined a number of states that have recently expanded the definition of personal information to trigger certain notice requirements when an individual's ''user name or email address'' is compromised along with either a ''password or security question and answer that would permit access to an online account.'' For incidents that only impact usernames and passwords, Illinois allows entities to provide notice to affected individuals simply by sending an email or other notice directing the individual to ''promptly change his or her user name or password and security question or answer'' and to take appropriate steps to protect all accounts for which they use the same log-in credentials.

Definition of personal information expanded to include health and biometric data. Illinois further expanded how it defines personal information to require notice when an individual's name is compromised in combination with their medical information, health insurance information or unique biometric data (such as fingerprint, retina or iris image). ''Medical information'' is broadly defined to include ''any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional,'' including ''information provided to a website or mobile application.''

Until recently only three states either allowed or required regulator notification to be made through submission of an online form. Now, seven states allow it.

Gramm–Leach–Bliley exemption added. Any entities that are ''subject to and in compliance with the standards established pursuant to Section 501(b) of the Gramm–Leach–Bliley Act'' are deemed to be in compliance with the statute. Section 501(b) of the GLB Act is the ''Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice.''

HIPAA exemption added – but notice to Illinois attorney general required. Any ''covered entity or business associate'' that is ''subject to and in compliance with the privacy and security standards'' for protecting personal health information under Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HI-TECH) are deemed to be in compliance with the statute. Importantly, if an entity is required to provide notice of an incident to the Secretary of Health and Human Services pursuant to HI-TECH, the entity must also notify the Illinois attorney general of the incident. Notably, the Illinois breach notification statute currently does not otherwise require notice to the Illinois attorney general (unless the breached entity is a state agency).

Nebraska—Effective July 21, 2016 (Neb. Rev. Stat. § § 87-802, 87-803, 87-804)

Limiting the encryption safe harbor. Similar to California and Illinois, Nebraska updated its law to require notification when encrypted data is compromised along with ''the confidential process or key'' that could be used to render the data readable or usable. Previously, Nebraska required notice only when ''unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information'' was involved.

Username + password incidents trigger notice obligations. Similar to Illinois, Nebraska updated its law to expand the definition of personal information to include ''a user name or email address, in combination with a password or security question and answer, that would permit access to an online account.'' Unlike Illinois, Nebraska's law does not maintain relaxed notification standards for breaches involving such information.

Requirement to notify attorney general. Nebraska updated its law to require that if notice is required to any Nebraska residents, notice must also be sent to the state attorney general. The notice must be provided to the attorney general ''not later than the time when notice is provided'' to the affected Nebraska residents. Importantly, the requirement to notify the attorney general applies regardless of the number of affected Ne-

  PVLR ISSN 1538-3423

braska residents. Some states only require notice to state regulators if a certain threshold number of state residents are impacted (e.g., California only requires regulator notice for incidents involving more than 500 residents).

Oregon—Effective Jan. 1, 2016 (ORS § § 646.607, 646A.602, 646A.604, 646A.622)

Biometric, health insurance and medical information trigger notice obligations. Oregon expanded the definition of personal information to require notice when an individual's name is compromised in combination with ''data from automatic measurements of a consumer's physical characteristics . . . that are used to authenticate the consumer's identity in the course of a financial transaction or other transaction.'' Oregon also expanded the definition to include ''a consumer's health insurance policy number or health insurance subscriber identification number in combination with any other unique identifier that a health insurer uses to identify the consumer'' and ''any information about a consumer's medical history or mental or physical condition or about a health care professional's medical diagnosis or treatment.''

Requirement to notify attorney general. Oregon updated its law to require notice of a breach to the state attorney general. Oregon limited this requirement to breaches in which the number of residents to whom notice must be sent exceeds 250.

Notice not required if subject ''unlikely to suffer harm.'' Oregon law provides an exemption from notification based on the risk of harm to the subject of the breach. Previously, the standard for this exemption was ''no reasonable likelihood of harm,'' but Oregon law now provides an exemption from notification when the subject of the breach is ''unlikely to suffer harm.''

HIPAA exemption added. Oregon added an exemption from breach notification for HIPAA-covered entities, provided that the entity sends the state attorney general a copy of specified regulator notifications required by HIPAA and a copy of any notice required by the Oregon law. The exemption does not state that it also applies to business associates.

Violation of data breach law now an unlawful practice. Finally, the Oregon law now specifies that a violation of the data breach law qualifies as an unlawful practice, allowing the attorney general or the district attorney of any county in which a violation occurs to bring enforcement proceedings.

Rhode Island—Effective July 2, 2016 (11 R.I. Gen. Laws Ann. § 11-49.3)

Notification letters to include number of impacted Rhode Island residents. Rhode Island became the first state to require that the number of impacted state residents be included in all notice letters sent to its residents. While several states require that information on the number of impacted individuals be included in notice letters sent to state regulators, this is the first law requiring such information be provided to impacted individuals. Practically, this will require businesses to customize notification letters when Rhode Island residents are impacted, adding an extra layer of complexity to the notification process for multistate breaches.

Requirement to cooperate with law enforcement investigations. Somewhat buried in the updated statute is the obligation for any entity to ''cooperate with federal, state, or municipal law enforcement in its investigation of any breach of security or unauthorized acquisition or use, which shall include the sharing of information relevant to the incident; provided[,] however, that such disclosure shall not require the disclosure of confidential business information or trade secrets.''

Limiting the encryption safe harbor. Like California, Illinois and Nebraska, Rhode Island updated its statute to clarify that notice is required when encrypted data is acquired along with information necessary to permit access to the data. The statute now provides that ''data shall not be considered to be encrypted if it is acquired in combination with any key, security code, or password that would permit access to the encrypted data.''

Expanded requirements for implementation of reasonable security practices. Rhode Island previously required that businesses that owned or licensed ''unencrypted personal information'' must implement and maintain reasonable security procedures related to the data. The statute now requires that entities that store, collect, process, maintain, own or license personal information on Rhode Island residents ''implement and maintain a risk-based information security program that contains reasonable security procedures and practices appropriate to the size and scope of the organization; the nature of the information; and the purpose for which the information was collected'' to protect the data. Like Illinois, the Rhode Island statute now requires that if personal information is to be shared with third parties, the contract with that party must require the third party to implement reasonable security practices to protect the data.

Definition of personal information expanded to include email address + password and health data. The updated Rhode Island statute requires notice when an individual's name is compromised along with ''medical or health insurance information''—both ''medical information'' and ''health insurance information'' are broadly defined. The statute also requires notice when an individual's name is compromised along with log-in credentials to certain accounts; specifically, notice is required when a name is compromised alongside an ''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.''

Specific penalties for violations. Rhode Island now allows the state attorney general to bring an action against companies that violate the statute. The statute provides that each ''reckless violation'' carries a penalty of not more than $100 ''per record,'' while each ''knowing and willful violation'' carries a maximum penalty of $200 per record. By way of example, a failure to notify 2,000 Rhode Island residents of a data breach could carry a maximum $400,000 penalty if the failure to notify was knowing and willful.

Requirement to notify attorney general Rhode Island's updated statute requires notification to the state attorney general if more than 500 Rhode Island residents are notified of an incident. Notice to the three major credit reporting agencies (i.e., Equifax, Experian and TransUnion) is also required if more than 500 Rhode Island residents are notified of a single incident.

Four states (California, Illinois, Nebraska and Rhode Island) implemented similar limitations to their encryption safe harbor protections related to data breaches.

Tennessee—Effective July 1, 2016 (T.C.A. § 47-18-2107)

Apparent removal of encryption safe harbor. One seemingly important change to the Tennessee statute was that it removed the word ''unencrypted'' from its definition of a ''breach,'' which seemed to indicate that Tennessee was removing its encryption safe harbor protection. Originally, the statute read that notice was required when there was an ''unauthorized acquisition of unencrypted computerized data that materially compromises the security, confidentiality, or integrity of personal information,'' but the amended statute removed the requirement that the computerized data at issue (i.e., the personal information) be unencrypted.

While that change appeared critical, in fact the statute's existing definition of personal information was unchanged, defining the term as an individual's name in combination with a secondary data element ''when either the name or the data elements are not encrypted.'' So if both the name and secondary data elements were encrypted, the data would not satisfy the definition of personal information, and therefore a breach triggering notice obligations would not have occurred. If, however, either the name or the secondary data elements were unencrypted, notice would be required under Tennessee law. For example, notice would potentially be required if individuals' names were compromised alongside their Social Security numbers if their names were unencrypted but their Social Security numbers were encrypted. About a dozen additional states define personal information in a similar manner where the compromise of an individual's unencrypted name and an encrypted secondary data element could trigger notice obligations.

Tennessee's amended statute provides a good example of the importance of closely reading an entire breach notification statute to understand what obligations it imposes.

Trends in Statutory Updates and Other Crucial Developments

More state regulators posting notices online and allowing for notice by submission of online form. As of 2015, only a handful of states posted security breach notifications sent to impacted individuals on state-operated websites (for some time only California and New Hampshire made such postings). Now, 11 states post breach notifications publicly. In addition, until recently only three states either allowed or required regulator notification to be made through submission of an online form. Now, seven states allow or require regulator notice to be made through submission of an online form or by sending a form via email . These trends show that state legislatures and regulators continue to streamline the process of data breach notification. This streamlining may continue into 2017 and beyond as other states amend their notification statutes and processes.

Closing the loophole on compromised encrypted data. This year four states (California, Illinois, Nebraska and Rhode Island) implemented similar limitations to their encryption safe harbor protections related to data breaches. The changes now require notification, for example, in cases where an encrypted laptop was stolen if the owner of the laptop left a note on the laptop with the username and password to bypass encryption protections. Under many state data breach statutes (and in the prior versions of these four state statutes), this scenario would not require notification.

Notice for username + password incidents and health or biometric data incidents on the rise. California and Florida were traditionally the only two states to require notice when an individual's username or email address and password (i.e., their log-in credentials) were impacted in a data breach. In the last few years, Nevada and Wyoming added somewhat similar requirements. This year Illinois, Nebraska and Rhode Island all implemented similar requirements, indicating that compromises of log-in credentials is a concern of state legislators and more states may adopt similar measures. In addition, Illinois, Oregon and Rhode Island each expanded the definition of personal information to require notice when certain forms of health or biometric data are compromised. The Illinois and Oregon statutes require notice for breaches involving biometric information, such as retina or fingerprint scans, and all three statutes require notice for breaches involving health insurance and medical information.

Not all username + password notice requirements are created equal. On Jan. 1, Illinois will join three other states (California, Florida and Nebraska) in requiring some form of notification when log-in credentials alone are compromised. When only log-in credentials are compromised, Illinois will allow entities to provide a limited notification to affected individuals via email that will inform them of the need to change the log-in credentials for the affected account and any other account that uses the same credentials. This form of limited notification is available in California as well, while Florida and Nebraska each require that the notice for such incidents comply with the same content and other requirements in place for data breaches involving other types of personal information. Nevada, Wyoming and now Rhode Island also require notification in some cases where log-in credentials are compromised. These states, however, only require notice when an individual's log-in credentials are compromised in conjunction with the individual's name. It is unclear if that was an intentional decision on the part of the legislatures or a result of unartful drafting.

  PVLR ISSN 1538-3423

Conclusion

The flurry of amended breach notification statutes has added a few more squares to the patchwork of state laws in this space. The specific amendments are a good reminder that, while there are broad, overarching consistencies among the state statutes, there are nuances that can dramatically alter an entity's notification obligations depending on the particular facts of the incident and which states' laws may be impacted. Importantly, the same facts can result in different obligations in different states.

Tennessee's amended statute provides a good example of the importance of closely reading an entire breach notification statute to understand what obligations it imposes. When Tennessee amended its statute and removed the word ''unencrypted'' from the definition of breach, several news outlets and law firms incorrectly stated that Tennessee had removed the encryption safe harbor from its statute. In reality, Tennessee had only modified its encryption protections. Other states' breach notification statutes, such as Wyoming and North Carolina, are confusingly drafted and further demonstrate the need for careful analysis.

A quick reading of the Wyoming law would suggest that notice is required for breaches involving nonsensitive information such as an address or telephone number, while a similar review of the North Carolina law indicates notice is required when names and email addresses alone are compromised. A careful analysis of the statutes, however, reveals that notice is not actually required in those states for such breaches. We expect 2017 to bring a myriad of amended statutes, all of which will require review with a fine-tooth comb to truly understand and appreciate their nuances.