MAYER·BROWN

Staying Informed About State Data Breach Laws

Scenario

A growing consumer products company is expanding its sales from brick and mortar stores to the Internet. The general counsel, who is charged with overseeing information governance at the company, is interested in keeping abreast of state data breach laws as the company grows and expands into new markets.

State Data Breach Laws

Several US states have recently passed or proposed new or amended data breach notification laws. As a result, there are now 47 states that have laws requiring businesses to notify individuals when data security breaches compromise their personal information. Enacted and proposed changes range from a broader definition of "personal information" to expanding the notification requirement to include all affected individuals rather than just affected state residents. The following is a summary of recently enacted breach notification laws, as well as other proposed laws being considered.

Kentucky: Protection for Student Data in the Cloud

Kentucky's new breach notification law became effective on July 15, 2014. It differs from other state breach notification laws in that it also provides protection for student data that is stored in the cloud. Cloud computing service providers should be aware of the new requirements, as they must certify in their agreements with educational institutions that they will comply with these provisions.

Student data means any information "in any medium or format" that concerns a student and is created or provided by the student in the course of their use of the cloud computing services or "by an agent or employee of the educational institution." Student data includes names, email addresses and messages, phone numbers, photos and other unique identifiers relating to the student. The law prohibits cloud computing service providers from processing student data "for any purpose other than providing, improving, developing or maintaining the integrity" of their computing services, unless the parents give express permission. Cloud computing service providers also may not process student data for advertising purposes, nor sell, disclose or otherwise process student data for any commercial purpose.

Florida: Expanded Definition of Personal Information

Florida recently amended its data breach notification law, which became effective on July 1, 2014.

The Florida Information Protection Act of 2014 replaces Florida's current breach notification statute and imposes several new requirements on covered entities. The amended law expands the law's definition of personal information to also include usernames and email addresses in combination with passwords or security questions and answers that permit access to an online account (similar to California's recently amended law, discussed below), health insurance policy numbers and medical history. The definition of a breach has also been expanded from an "unlawful and unauthorized acquisition" of personal information to a broader "unauthorized acquisition" of such information.

The amended law requires businesses to notify affected individuals within 30 days of a breach (unless good cause is shown, in which case a business may receive an additional 15 days to provide notice). This is one of the shortest individual notification deadlines among state data breach notification laws. Businesses must also notify the Florida Attorney General within 30 days if a breach affects 500 or more individuals and provide copies of forensic reports and "policies regarding breaches" to the Florida Attorney General upon request. Additionally, if a business is required to notify more than 1,000 individuals at a single time as a result of a breach, it must also notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.

Florida's amended law also now requires businesses to use "reasonable measures" to protect and securely dispose of personal information.

Iowa: Expanded Scope that Includes Paper Documents

SF 2259, which was signed into law in April 2014, modifies Iowa's breach notification law in two significant ways. First, the legislation expands the definition of "breach of security" to include the unauthorized acquisition of personal information maintained in any medium—including on paper—that was transferred to that medium from computerized form. Second, the law requires covered businesses to notify the Iowa Attorney General's office if a security breach affects more than 500 Iowa residents. This written notice must be given within five business days after notifying consumers of the breach. The amended law took effect on July 1, 2014.

Minnesota: Proposed Law Expands Scope of Notification and Would Make Businesses Liable for Other Data-Breach-Related Costs

Minnesota is proposing legislation that would considerably expand the scope of its current breach notification law. Minnesota's current law requires notification of security breaches to state residents when their unencrypted personal information has been compromised. The proposed legislation would expand notification requirements to any individual whose unencrypted personal information was compromised by a covered entity's security breach. Entities conducting business in Minnesota would potentially be required to notify individuals across the country of breaches. Additionally, these notifications would need to occur within 48 hours of discovery or notification of a security breach. The Minnesota bill, if passed, would also make businesses responsible for other costs related to data breaches. After giving notice to individuals, businesses would need to provide one year of credit monitoring services at no charge to those affected by the breach. Retailers or wholesalers of consumer goods and services would be required to provide each individual a $100 gift card for future use, valid for at least one year. Finally, businesses would need to reimburse individuals who incur any charges or fees as a result of the breach.

California: Proposed Law Increases Encryption Standard and Requires Businesses to Provide Theft Prevention and Mitigation Services

California recently amended its data breach notification statute to expand the definition of

personal information to include online account information, such as an email address and password. California is now considering amending its data breach statute further, with the Consumer Data Breach Protection Act (AB 1710). The current California law does not require businesses to notify individuals affected by security breaches if the data is encrypted (using any encryption method). However, if AB 1710 is passed in its current form, it will require businesses to notify California residents of any data breach unless the data is encrypted "in conformance with the Advanced Encryption Standard of the National Institute of Standards and Technology, Federal Information Processing Standards Publication 197, as amended from time to time." This higher encryption standard, along with the requirement that businesses provide theft prevention and mitigation services to affected persons after a breach, aims to address increased retailer breaches in a manner similar to Minnesota's proposed approach. AB 1710 would also prohibit the sale, advertisement for sale or offer to sell any individual's Social Security number. In addition, the proposed law would require retailers and other businesses to notify consumers of a breach at the same time they notify data owners. AB 1710 previously had provisions that would have made businesses liable for breach notification and card replacement costs, but these provisions have since been removed.

New Mexico: Proposed Law Includes Payment Card Breach Notification Requirements

New Mexico, one of three states that currently do not have breach notification laws, has proposed legislation that would require businesses to notify New Mexico residents of security breaches involving their unencrypted personal information within 45 days after discovering a breach. In cases where a breach would require notice to more than 1,000 residents, businesses would also need to notify the New Mexico Attorney General and consumer reporting agencies. The proposed law also contains payment card breach notification requirements. Credit or debit card issuers would need to notify all merchants to which credit or debit card numbers were transmitted, if there was a breach of payment card information.

Conclusion

Because data breach notification laws are constantly changing, businesses should consider the statutes of all states in which they do business or of whose residents they have personal information. Businesses without incident response plans should consider developing one, and businesses with such plans should consider annually reviewing and updating their plans and testing aspects of such plans by running simulation events. These plans can help reduce breach investigation and response times, which is essential given the tight notification time frames now required by some states.

In addition, businesses should consider encrypting all personal information wherever possible or practical, not just the information currently required by data breach notification laws, since these laws are constantly being updated to include more elements of personal information within their scope. To comply with new state requirements, businesses should also consider implementing a data destruction program to securely destroy data that is no longer needed.

For inquiries related to this Tip of the Month, please contact Rebecca Eisner at reisner@mayerbrown.com, Lei Shen at lshen@mayerbrown.com or Kim Leffert at kleffert@mayerbrown.com

Learn more about Mayer Brown's Electronic Discovery & Information Governance practice or contact Anthony J. Diana at adiana@mayerbrown.com, Eric B. Evans at eevans@mayerbrown, Michael E. Lackey at mlackey@mayerbrown.com or Edmund Sautter at esautter@mayerbrown.com.

Please visit us at www.mayerbrown.com.