The More Things Change... More Amendments to State Breach Notification Laws

By: Mary Ellen Callahan and Heidi Wachs

Connecticut

On June 1, 2015, the Connecticut General Assembly unanimously approved amendments to the state's current data breach notification law. Effective October 1, 2015 when, as expected, it is signed by Governor Daniel Malloy, the bill sets a 90-day deadline for companies to report data breaches to affected residents as well as the state Attorney General. The bill also requires companies to provide victims with one year of identity theft protection, making Connecticut the first state in the country to require identity theft protection. California enacted a similar law this January, requiring a full year of protection if a business elects to offer credit monitoring.

Effectively, the new identity theft protection requirement will partially put into law what has been common practice in the state. Connecticut Attorney General George Jepsen routinely requests that companies provide identity theft protection of one or two years, as he did after the Anthem breach. Jepsen has stated that he will continue to request companies to provide two years of protection for breaches of "highly sensitive information," such as Social Security numbers. He considers the new requirements to set a "floor," not a ceiling, to the length of time identity theft protection will be required.

Montana, Nevada, North Dakota, Washington and Wyoming

Connecticut's move to toughen its data breach notification requirements is the latest in a series of updates to state breach notification laws. Montana, Nevada, North Dakota, Washington, and Wyoming all approved updates to their laws earlier this year, each expanding the scope of notification once the laws come into effect:

- Montana's definition of "personal information" will now include names combined with medical information, taxpayer identification numbers, and IRS-issued identity protections PINs. Businesses will also have to simultaneously submit a copy of the data breach notice to the state Attorney General, specifying how many Montana residents were affected. In some instances, businesses will be required to notify the Commissioner of Insurance as well.

- Nevada's definition of "personal information" will widen to include usernames and emails in conjunction with passwords, access codes, or security questions.

- North Dakota's data breach law will apply to any entity that "owns or licenses" personal information of state residents, not only those entities that conduct business in the state. Compromised employee identification information, however, will only trigger the law's notification requirement if combined with passwords or codes.

- Washington's law will impose a 45-day deadline to report breaches to affected residents and the state attorney general, if the breach affects over 500 residents. Notification requirements will also apply to hard copy as well as computerized data, including encrypted data whose encryption keys have been compromised.

- Wyoming adopted a number of amendments that will significantly expand its definition of "personal information." Names combined with credit or debit card numbers, government-issued ID card numbers, birth or marriage certificates, medical or health insurance information, biometric information, taxpayer identification numbers, as well

as username or email addresses with passwords or security question answers will all become triggers for notification. In addition, the law adopts a number of content requirements for data breach notices. Notices must include a toll-free contact number, a list of the types of personal information affected, a general description and date of the breach, a description of the actions taken to prevent future breaches, advice to consumers on how to protect their information post-breach, and whether a law enforcement investigation had delayed the breach notification. Wyoming also took the unusual step of removing a data element from its definition of personal information, removing "place of employment" and "employee identification number" after employers complained.

These changes reflect the increasing complexity of complying with state data breach notification laws, which have created a confusing patchwork of legal triggers and duties across the country. As a result, lawmakers and practitioners might be turning with renewed enthusiasm to the possibility of enacting a federal data breach notification law. Recently introduced bills like the Consumer Privacy Protection Act of 2015 and the Data Security and Breach Notification Act of 2015 are still making their way through Congress. Some opponents worry that these bills would weaken strong state laws with more stringent notification requirements. The Data Security and Breach Notification Act, for example, only requires notification in the event of "identity theft, economic loss or economic harm." Others worry that these bills might impose more onerous requirements on businesses. Several other bills, including the Personal Data Notification & Protection Act, have been the subject of comparable concerns and ongoing debate.

As the pressure mounts for a nationwide standard for data breach notification, states are continuing to revise their notification laws. Alabama, one of only three states without a notification law on the books, is currently considering data breach legislation. Meanwhile, amendments to existing state legislation are pending in at least 13 other states.

In light of these impending changes to state breach notification laws, companies should review and update their programs and policies, including seeking help from outside counsel as necessary. Incident response and breach notification plans should reflect the most up-to-date notification requirements, including which Attorneys General must be notified and any applicable timelines. In addition, companies may want to review their information classification policies to ensure that as definitions of personal information expand, so do their policies and controls for the appropriate handling of the enumerated data elements.

Thanks to Daniela L. Nogueira for her help with this Alert.

Contact Us

Mary Ellen Callahan, Partner, Jenner & Block

Phone: 202.639.6064 Email: mecallahan@jenner.com DOWNLOAD V-CARD

Heidi Wachs, Special Counsel, Jenner & Block

Phone: 202.639.6081 Email: hwachs@jenner.com DOWNLOAD V-CARD