More data breaches mean more changes to data breach notification laws in 2018

JOELLE DVIR | DATA PRIVACY SOLUTIONS | MAR 02, 2018

It's been a busy 2018 for the constantly evolving landscape of data breach notification laws. Currently, 48 states and the District of Columbia have enacted data breach notification statutes requiring private or governmental entities to notify individuals of security breaches when personally identifiable information is involved. Only South Dakota and Alabama remain without data breach notification statutes; however, that may soon change in South Dakota.

SOUTH DAKOTA

On Jan. 23, 2018, the South Dakota Senate Judiciary Committee passed a bill (S.B. 62) that creates a breach notification requirement that applies to any person or business conducting business in South Dakota, who owns or retains computerized personal or protected information of South Dakota residents. The bill requires disclosure of a breach to any affected South Dakota resident, whose personal or protected information was, or is reasonably believed to have been, acquired by an unauthorized person, within 60 days from the discovery or notification of the breach, unless a longer time frame is needed by law enforcement.

If the breach affects more than 250 South Dakota residents, the bill also requires disclosure to the attorney general and all consumer reporting agencies, and any other credit bureau or agency that compiles and maintains files on consumers on a nationwide basis. South Dakota Attorney General Marty Jackley cited the massive Equifax Inc. and Target Corp. data breaches as motivation for this bill and stated the bill was "an important step to protect consumers and to assist law enforcement in its investigation of major data breaches."

If South Dakota enacts this bill, Alabama would be the only state without a data breach notification law, however the Alabama attorney general's office has indicated that it is optimistic that Alabama will enact a breach notification statute in 2018.

COLORADO

Lawmakers in Colorado are setting their sights on more stringent breach notification laws. On Jan. 22, 2018, a bipartisan group of Colorado legislators introduced a bill (H.B. 1128), that would strengthen the state's notification requirements, giving any individual or company that conducts business in Colorado a 45-day deadline to provide notice to affected individuals, and no more than seven days to notify the attorney general if more than 500 people are affected.

Notably, the Colorado bill requires entities to implement "reasonable security procedures" to protect consumers' personal information, but does not give any guidance on what these "reasonable" security procedures would look like. The bill also requires any company that maintains personal consumer data to have a written policy outlining how it will securely destroy the data if it is no longer needed. Similar to the South Dakota bill, if more than 1,000 residents are affected, the bill requires disclosure to all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.

NORTH CAROLINA

In North Carolina, the attorney general and a legislator jointly introduced legislation that would give organizations only 15 days to report a data breach to consumers and the attorney general. This shortened time frame would give consumers a greater chance of taking protective measures to prevent identity theft before it occurs. The breach notification would include ransomware attacks when personal information is accessed, but not necessarily acquired. The bill would also allow consumers to place and lift a credit freeze on their credit report at any time, for free, preventing a hacker from using the consumer's stolen data to open a fraudulent credit line. If passed, it would give North Carolina one of the toughest breach notification laws in the United States.

MARYLAND

Maryland's amended data breach notification law went into effect on Jan. 1, 2018. The modifications include an expansion of the definition of personal information to include biometric information. Biometric information is defined under the statute as "any automatically generated biologic measurements, such as a fingerprint, voice print, genetic print, retina or iris image, or other unique biological characteristic, that can be used to uniquely authenticate an individual's identity." Maryland also changed its notification requirement from "as soon as reasonably practicable", to no more than 45 days after learning of the breach. If notification is delayed due to an investigation by law enforcement, notification is required within 30 days after law enforcement determines that notification will not impede the investigation.

Maryland's statute includes a requirement that the business "implement and maintain reasonable security procedures and practices", but fails to detail what those procedures would look like. However, an earlier version of the amended bill included a specific list of procedures for businesses to follow, including a requirement to: maintain a written information security policy, designate responsible parties to oversee an information security program, conduct risk assessments and address safeguards to control the identified risks, ensure that service providers adequately safeguard personal information and implement changes based on periodic evaluations. Although not enacted, these procedures provide a good framework for what businesses should consider when devising their data privacy plan.

Now is the time to update your incident response plans to reflect these rapidly changing breach notification obligations. McDonald Hopkins will continue to monitor this space to provide the most up-to-date information available.

JOELLE DVIR

Read More