Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

South Dakota Breach Notification Law Breaks New Ground

By **Caleb Skeath and Calvin Cohen** (March 29, 2018, 12:30 PM EDT)

Caleb Skeath

Calvin Cohen

Last week, South Dakota became the 49th U.S. state to enact a data breach notification law with the passage of S.B. 62, which sets forth requirements for notifying state residents, the state attorney general, and major consumer reporting agencies in the event of a breach. The law, which will take effect on July 1, 2018, parallels many recently passed or amended state data breach notification laws through its inclusion of an expansive definition of "personally identifiable information" and an explicit deadline for notifying affected residents. However, a few elements of the law push further than comparable laws from other states and have the potential to shift companies' data breach notification practices.

Under the new law, any person or business conducting business in South Dakota that owns or licenses computerized "personal or protected information" of South Dakota residents must provide notice of the breach unless certain exceptions apply. A "breach" occurs when personal or protected information was, or is reasonably believed to have been, acquired by an unauthorized person. Notably, the law defines an "unauthorized person" to include not only individuals who are not authorized to acquire or disclose personal information, but also individuals who are authorized to do so but have acquired or disclosed personal information "outside the guidelines for access o[r] disclosure established by the information holder." This specific addition to the law could impact decision-making processes for businesses who encounter potential data security incidents that parallel the characteristics set forth in the statute.

The law defines a breach to include the disclosure of personal or protected information that is unencrypted, or encrypted if the encryption key is also acquired. By implication, a breach of encrypted information without an associated compromise of the encryption key will not be covered within this definition. In order to qualify as encrypted, however, data must be rendered "unusable, unreadable, or indecipherable" either "without the use of a decryption process or key" or in accordance with the Federal Information Processing Standard 140-2 in effect on Jan. 1, 2018. Although it is not free from doubt, this provision indicates that compliance with FIPS may not be strictly required but may instead represent a more explicitly defined safe harbor that companies can implement to take advantage of this exception from disclosure requirements.

The concept of "personal or protected information" expands the scope of the information this law covers beyond other comparable state data breach notification laws. The definition of "personal

information" parallels other state data breach notification laws by covering an individual's name in conjunction with a Social Security number, driver's license number (or other government-issued identification number), or an account, credit card, or debit card number in combination with any required security code, access code, password, routing number, PIN or any additional information that would permit access to a person's financial account. However, the definition also covers a name in conjunction with "health information" (as defined under the Health Insurance Portability and Accountability Act) or an employer-assigned identification number in combination with any required security code, access code, password, or biometric data used for authentication purposes.

"Protected information," on the other hand, does not need to be disclosed in connection with an individual's name. South Dakota's new law joins several other states that have recently begun to require disclosure of breaches of a user name or email address, in combination with a password, security question answer, or other information that permits access to an online account. However, South Dakota's new law also goes farther than other state laws in defining "protected information" to include an account 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, even in the absence of an individual's name. Although most state data breach notice laws only cover such information if disclosed in connection with an individual's name, South Dakota's law will require disclosure of a breach of this information regardless of whether individuals' names are involved.

South Dakota also joins a recent trend among other state data breach notification laws in setting explicit deadlines for providing notification to affected individuals, the state attorney general and major consumer reporting agencies. Under the law, an information holder must notify affected individuals of the breach by mail, email or substitute notification measures within 60 days after the discovery or notification of the breach. The law also requires an information holder to disclose the breach to the state attorney general if the breach involves more than 250 South Dakota residents. If an information holder "reasonably determines," after an "appropriate investigation," that the breach will not likely result in harm to affected individuals, notification to the individuals is not required, but the information holder must notify the attorney general and maintain documentation of this determination in writing for three years. The notification can also be delayed if a law enforcement agency determines that it will impede a criminal investigation, but must be provided within 30 days after the agency determines that it will not compromise the investigation.

If an information holder must notify individuals of a breach, the law states that the information holder must also notify "all consumer reporting agencies," as defined under the Fair Credit Reporting Act, and "any other credit bureau or agency that compiles and maintains files on consumers on a nationwide basis." This expansive requirement differs significantly from other state data breach notification laws, which often only require notification of the three major consumer reporting agencies if a breach impacts more than a specific number of state residents (usually 1,000). No explicit time frame is required for either of these types of notifications.

The new law also includes "safe harbor" provisions for HIPAA- or Gramm-Leach-Bliley Act-regulated entities that notify affected South Dakota residents in compliance with applicable federal laws or regulations. For entities that fail to disclose a breach under the new law, however, such a failure could prove costly. Under the law, the state attorney general can prosecute "each failure to disclose" as a deceptive act or practice under state law and, in addition to any remedy provided for such acts or practices by state law, may recover a civil penalty of up to $10,000 per day per violation, in addition to attorneys' fees and costs.

South Dakota's new law may represent the next step in the evolving landscape of compliance with varying provisions of state data breach notification laws, and several unusual provisions could complicate decision-making for businesses required to notify South Dakota residents.

Caleb Skeath and Calvin Cohen are associates in the Washington, D.C., office of Covington & Burling LLP.