Banking and Finance Law Daily Wrap Up, TOP STORY—South Dakota enacts security breach notification requirements, (Mar. 27, 2018)

Banking and Finance Law Daily Wrap Up

Click to open document in a browser

By Charles A. Menke, J.D.

South Dakota has enacted legislation requiring information holders to notify state residents affected by an unauthorized acquisition of unencrypted computerized data, or encrypted computerized data and the encryption key, by any person that materially compromises the security, confidentiality, or integrity of personal information or protected information. The legislation (S.B. 62), which was introduced at the request of the state's attorney general, Marty Jackley, makes South Dakota the 49th state to enact security breach protections for consumers.

Personal and protected information. "Personal information" subject to protection consists of an individual's first name or first initial and last name in combination with any one or more of the following data elements:

- Social Security number;
- driver license number or other unique government issued identification number;
- account, credit card, or debit card number, in combination with any required security code, access code, password, routing number, personal identification number, or any additional information that would permit access to a person's financial account;
- health information as defined under federal regulation; or
- an identification number assigned to a person by the person's employer in combination with any required security code, access code, password, or biometric data.

Additional "protected information," includes:

- a user name or email address, in combination with a password, security question answer, or other information that permits access to an online account; and
- 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.

Notification requirements. An information holder—any person or business that conducts business in South Dakota and that owns or licenses computerized personal or protected information of South Dakota residents—must disclose by written notice, electronic notice, or substitute notice a security breach of personal information within 60 days after the breach was discovered. If the breach exceeds 250 South Dakota residents, the information holder must also notify the South Dakota attorney general within 60 days.

Notification may be delayed if a law enforcement agency determines that it will impede a criminal investigation. If the notification is delayed, the notification must be made within 30 days after the law enforcement agency determines that notification will not compromise the investigation. Notification is not required if, following an appropriate investigation and notice to the attorney general, it is determined that the breach will not likely result in harm to the affected individuals.

Enforcement. The state's attorney general is charged with enforcing the Act, and may prosecute a failure to provide notification as required as a deceptive act or practice. In addition, the attorney general may bring an action to recover on behalf of the state a civil penalty of up to $10,000 per day per violation, and may recover attorney's fees and costs associated with the action.

Compliance with federal law. An information holder that is regulated by federal law or regulation, and that maintains procedures for a breach of system security pursuant to the laws, rules, regulations, guidance, or guidelines established by its primary or functional federal regulator is deemed to be in compliance with the South

© 2018 CCH Incorporated and its affiliates and licensors. All rights reserved.

Dakota requirements if the information holder notifies affected South Dakota residents in accordance with the provisions of the applicable federal law or regulation.

Effective date. The law (S.B. 62) takes effect July 1, 2018, and leaves Alabama as the only state that has not enacted some type of breach notification law, although that distinction appears to be fleeting. The Alabama House of Representatives recently passed an amended version of security breach legislation—the Alabama Data Breach Notification Act (S.B. 318)—that previously cleared the state's Senate. The legislation returns to the Alabama Senate, which must now vote on whether to concur.

MainStory: TopStory AlabamaNews ConsumerCredit CyberPrivacyFeed FairCreditReporting IdentityTheft Privacy SouthDakotaNews StateBankingLaws

© 2018 CCH Incorporated and its affiliates and licensors. All rights reserved.