Publications
May 18, 2018
SECURITY BREACH NOTIFICATION CHART - South Dakota

S.D. Code 22-40-20 ***et seq.***

South Dakota S.B. 62 (signed into law March 21, 2018)

Effective July 1, 2018

Application. Any person or business that conducts business in South Dakota, and that owns or licenses computerized personal or protected information of residents of SD (Entity).

Security Breach Definition. The 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 or protected information.

- Good-faith acquisition of personal or protected information by an employee or agent of an Information Holder is not a security breach, provided that the information is not used for a purpose unrelated to the business or subject to further unauthorized use.

Notification Obligation. Any Entity that discovers or is notified of a breach of system security must notify affected individuals.

- Notice is not required if, following appropriate investigation and notification to the Attorney General, the Entity reasonably believes the incident will not result in harm to affected individuals. The Information Holder shall document this determination in writing and keep record of this documentation for 3 years.

Attorney General Notification. If the number of affected individuals exceeds 250 residents, the Entity must notify the Attorney General.

Notification to Consumer Reporting Agencies. The Entity must notify, without unreasonable delay, all nationwide consumer reporting agencies.

Timing of Notification. Notice must be given no later than 60 days from when the Entity discovers or is notified of a breach.

Personal Information Definition. SD's statute covers both "personal information" and "protected information."

"Personal Information" means a person'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's license number or any other unique identification number created or collected by a government body;
- Account number, credit card number, or debit card number in combination with any required security code, access code, password, routing number, PIN, or any additional information that is necessary to access the financial account;
- Health information as defined in 45 CFR 160.103 (HIPAA);

- 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 generated from measurements or analysis of human body characteristics for authentication purposes;

The term does not include information that is lawfully made available to the general public from federal, state, or local government records or information that has been redacted, or otherwise made unusable.

"Protected information" includes:

- A username 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 and debit card number, in combination with any required security code, access code, or password that permits access to a person's financial account;

Notice Required. Notice may be provided by one of the following methods:

- Written notice;
- Electronic notice, if the electronic notice is consistent with the requirements for electronic records and signatures set forth in 15 U.S.C. § 7001 (E-Sign Act), or if the information holder's primary method of communication with the SD resident has been by electronic means.

Substitute Notice Available. Substitute notice is acceptable if notification will exceed $250,000, the affected class of persons to be notified exceeds 500,000 persons, or the Entity does not have sufficient contact information and the notice consists of each of the following:

- Email notice, if the Entity has the affected individual's email address;
- Conspicuous posting of the notice on the website of the Entity, if it has a website; and
- Notification to statewide media.

Exception: Own Notification Policy. An Entity that maintains its own notification procedure as part of its information security policy, and the policy is consistent with the timing requirements of the Act, is considered in compliance with the notification requirements of this Act if it notifies affected persons in accordance with its internal policy

Exception: Compliance with Other Laws.

- **Federal law.** An Entity subject to or regulated by federal laws, rules, regulations, procedures, or guidance (including the Gramm-Leach-Bliley Act and HIPAA) is considered in compliance with the Act as long as the Entity maintains procedures pursuant to the federal law requirements and provides notice to consumers pursuant to those requirements.

Other Key Provisions:

- **Delay for Law Enforcement.** Notice may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation. The Information Holder must provide notice within 30 days after the law enforcement agency determines notice will no longer impede a criminal investigation.
- **Attorney General Enforcement.** The Attorney General can bring an action for civil penalties under the Act.