Published on *The National Law Review* https://natlawreview.com

(Another) Federal Data Breach Notification Law Introduced in Congress

Article By:

Gregory Bautista

Jeremy T. Merkel

Senate Democrats have introduced a **third iteration** of a federal data breach notification bill, the Data Security and Breach Notification Act of 2017 (S.B. 2179). If passed into law, this bill would replace the patchwork of 48 separate state breach notification laws and standardize breach reporting requirements, which currently vary from state to state.

Introduced by Sen. Bill Nelson (D-FL) and cosponsored by Sen. Richard Blumenthal (D-CT) and Sen. Tammy Baldwin (D-WI), the Data Security and Breach Notification Act would apply to companies that acquire, maintain or use consumers' personal information. The bill's definition of "personal information" is slightly broader than the corresponding definition under many state laws, and includes, for example, Social Security Numbers on their own, and names in combination with the following identifiers:

- Government identification number, such as a driver's license or passport
- Unique biometric data, such as a finger print, voice recording or retina image
- User names and passwords for access to anything of value
- Any two of the following: home address or telephone number, mother's maiden name or date of birth.

Financial entities that are in compliance with the Gramm-Leach-Bliley Act or covered entities in compliance with the HIPAA Security Rule would not be covered.

Most notably, the bill requires that companies notify individuals and the Federal Trade Commission within 30 days of discovering a data breach that involves consumers' personal information. This is a significantly shorter notification period than most state laws, which require notification within 45 or 60 days, or even the HIPAA Breach Notification Rule, which requires breaches be reported no later than 60 days after detection. Where more than 5,000 individuals are affected, the credit reporting agencies

must be notified as well. Notice to a designated government entity also will be required in any of the following circumstances:

- The breach affects more than 10,000 individuals
- The breach involves a database containing the personal information of more than one million individuals
- The breach involves databases owned by the federal government
- The affected individuals are government employees or contractors involved in national security or law enforcement.

The designated government entity will provide the notices it receives to the U.S. Secret Service, the Federal Bureau of Investigation, the Federal Trade Commission, the attorney general of each state where affected individuals reside and the U.S. Postal Inspection Service if the breach involves mail fraud.

If a company can reasonably conclude that there is no risk of identity theft, fraud or other unlawful conduct as a result of the breach, it would be exempt from the bill's notification requirements. Under the bill, there is a presumption of no reasonable risk of identity theft or fraud if the data is rendered "unusable, unreadable, or indecipherable through a security technology or methodology" that is generally accepted by information security experts. The National Institute of Standards and Technology (NIST) is charged with identifying adequate security technologies and methodologies. Overall, as this risk-of-harm exemption is not currently available under all state laws, it represents a more business-friendly change and limits the risk of over-notification to consumers.

Additionally, the bill imposes significant penalties of fines and up to five years in prison on executives of companies that "intentionally and willfully" conceal and fail to report a data breach. This comes in the wake of highly publicized data breaches that saw companies delay notifying consumers that their personal and financial information had been compromised. States' attorneys general also have the right to bring a civil action on behalf of their residents to obtain civil monetary penalties of up to $11,000 per day for each day that the company is noncompliant.

The bill also would require companies to develop procedures to assess "reasonably foreseeable" system vulnerabilities and methods for disposing of data that is no longer being used through destruction or rendering it unreadable. The FTC would establish these new security standards and provide incentives to companies that implement technology that would render consumer data "unusable or unreadable if stolen during a breach."

National Law Review, Volume VII, Number 352