Securities
Regulation Daily

Wolters Kluwer

November 6, 2017

STRATEGIC PERSPECTIVES—After Equifax, a renewed focus on state and federal cybersecurity disclosure

By Anne Sherry, J.D.

Recent data breaches at Equifax and the Securities and Exchange Commission have renewed the spotlight on all aspects of cybersecurity, including disclosure. Shortly before the public revelations of these breaches, on August 17, Delaware's governor signed the first major revision to the state's data breach notification law since its 2005 enactment. Significantly, the new law, which will go into effect next April, requires "persons" (which includes individuals, business entities, and governmental entities) to notify Delaware residents whose information was compromised within 60 days of discovery—a significant departure from the "as soon as possible" standard of the previous law.

Equifax's disclosure six weeks after learning of the breach fits within that timeline, while the SEC has not made it clear when it learned of the 2016 EDGAR breach. Chairman Jay Clayton testified before a Senate committee that he was personally notified in August 2017; the agency publicly disclosed the incursion on September 20. It has since disclosed that the personal information of at least two individuals was compromised and that it has reached out to those individuals.

The new Delaware law applies to any "person" doing business in Delaware, not just entities based or incorporated in the state. Companies must also comply with a patchwork of state laws protecting residents in the states in which they do business. According to the National Conference of State Legislatures, Alabama and South Dakota are the only states without a security breach notification law.

While there is no data notification law at the federal level, these security breaches have renewed attention on the SEC's disclosure regime and whether it is sufficiently robust in the context of emerging cybersecurity threats. Some legislators maintain that the agency's existing 2011 guidance on cybersecurity is overdue for an update, and many are questioning whether materiality is the appropriate standard for determining whether a cyber incident must be made public. Chairman Clayton has dedicated new resources to cybersecurity, while at the same time reiterating that materiality is the touchstone of the agency's disclosure regime.

Delaware's Data Breach Notification Law

Governor John Carney signed House Substitute 1 for HB 180, which made significant changes to the text of the original bill, but moreover overhauled the state's existing data breach notification requirements entirely. When it goes into effect on April 14, 2018, the law will require a person to

notify affected Delaware residents of any breach of personal information, *unless* it determines after an investigation that the breach is unlikely to result in harm. Currently, persons need only notify residents after determining that personal information has been, or will be, misused.

"Personal information." The definition of "personal information" has been significantly expanded with the new amendments, although the law as enacted dials back the scope of protected information compared to the initial bill. Under both the current and new law, personal information includes social security numbers, driver's license numbers, and account or debit card numbers (in combination with codes or passwords that would permit access to a resident's financial account).

The amendments expand the definition to also include state or federal identification card numbers; credit card numbers (again only if in combination with an access code or password); passport numbers; usernames or email addresses in combination with a password or security question and answer; medical history or DNA profile; health insurance identifiers; biometric data used for authentication; and individual taxpayer identification numbers. HB 180 originally included marriage certificates; full birth dates and birth certificates; shared secrets and security tokens; and digital and electronic signatures. These types of information are not "personal information" under the Substitute Act.

The current law defines a security breach as involving "unencrypted computerized data." The new amendments go further by specifically stating that the unauthorized acquisition of data is not a breach of security to the extent that the personal information is encrypted, unless the acquired data includes (or is believed to include) the encryption key and the person that owns or licenses the encrypted information has a reasonable belief that the key could render the personal information readable or usable.

Notification requirements. Notice can be written, telephonic, or electronic. The person may also notify residents by substitute notice if the cost of individual notice would exceed $75,000 or if more than 100,000 Delaware residents were affected, or if the business lacks sufficient contact information to provide notice. To effect substitute notice, the person must provide electronic notice if residents' emails are available; post a conspicuous notice on its website, if it maintains one; and notify major statewide media, including newspapers, radio, television, and social media.

If email credentials are compromised, the person cannot comply with the law by sending notification to the compromised email address. Instead, the person must use another method of notice approved by the law or can deliver "clear and conspicuous notice … online when the resident is connected to the online account from an Internet Protocol address or online location from which the person knows the resident customarily accesses the account."

If more than 500 Delaware residents were affected in the breach, the Attorney General must also be notified no later than the residents are.

Identify theft protection. If the breach includes a social security number, the person must offer identity theft protection services and, if applicable, identity theft mitigation services at no cost to affected

residents for one year. This must include all information necessary for the resident to enroll, as well as information on how the resident can freeze his or her credit file. Identity theft protection services are not required if the person reasonably determines after an appropriate investigation that the security breach is unlikely to result in harm to the individuals whose information was compromised.

Compliance and enforcement. A person that maintains its own notice procedures as part of an information security policy may notify Delaware residents in accordance with those policies, as long as the procedures are otherwise consistent with the law's timing requirements. Persons regulated by state or federal law, including HIPAA and the Gramm Leach Bliley Act, may comply with the law by notifying affected Delaware residents in accordance with procedures maintained pursuant to the regulator's rules.

The Delaware Attorney General may bring an action in law or equity for violations of the law. The original text of HB 180 also provided a private right of action. This language was removed in the Substitute Bill, which states that: "Nothing in this chapter may be construed to modify any right which a person may have at common law, by statute, or otherwise."

Disclosure at the Federal Level

There is no federal data breach notification law. Recently, in the wake of the Equifax breach, lawmakers and investor advocates have renewed calls for the SEC to require registrants to publicly disclose when a data breach occurs.

The SEC's 2011 guidance on cybersecurity disclosure, put out by the Division of Corporation Finance, explains how cybersecurity fits in to the existing regime of disclosure of specific material events. Regulation S-K requires disclosure on Form 8-K of certain enumerated events. Outside of these affirmative, formal disclosure requirements, however, there is no general requirement that a company disclose information simply because it is material.

The guidance acknowledges the fine line between disclosing vulnerabilities and keeping investors informed. In line with the overarching materiality framework for disclosure generally, companies much disclose cyber incursions and cyber risks to the extent that they rise to the level of a specific threat or cost enumerated in Regulation S-K.

Specific material events. Accordingly, the guidance instructs that cyber incidents must be disclosed under Item 503(c) if they are "among the most significant factors that make an investment in the company speculative or risky." Disclosure may also be required in the Management's Discussion and Analysis (MD&A) if the costs or other consequences associated with a cyber incident or the risk of potential incidents "represent a material event, trend, or uncertainty that is reasonably likely to have a material effect on the registrant's results of operations, liquidity, or financial condition or would cause reported financial information not to be necessarily indicative of future operating results or financial condition." The breach may need to be disclosed in the "Description of Business," "Legal Proceedings," or financial statement disclosures, depending on the nature and severity of the incident.

There also may be required disclosures or accounting considerations relating to the costs of preventing and responding to cyber incidents, as well as the effectiveness of disclosure controls and procedures themselves. "For example, if it is reasonably possible that information would not be recorded properly due to a cyber incident affecting a registrant's information systems, a registrant may conclude that its disclosure controls and procedures are ineffective," according to the guidance.

Calls for SEC action. In testimony before the Senate Banking Committee shortly after the reveal of both the Equifax breach and the SEC's EDGAR breach, Chairman Clayton reaffirmed that the materiality standard is the touchstone of the SEC's disclosure system, to some pushback from senators who felt this was not a sufficiently robust response to an ever-growing threat. Mark Warner, the Virginia Democrat who serves as Vice Chair of the Senate Intelligence Committee, pointed out that Yahoo's systems were breached in 2016, affecting 500 million users, but the company did not feel the event was material enough to report. Since 2010, fewer than 100 companies have disclosed cyber incursions as material events, he added.

Industry watchdog group Better Markets urged the SEC to adopt an "Equifax rule" that would provide that a data breach is presumptively material. Only if there were "overwhelming and incontrovertible facts to the contrary" would disclosure be excused.

It is not the first time the SEC has faced heat about its cybersecurity requirements. Two years ago, Representatives Jim Langevin (D-RI) and Jim Himes (D-Conn) called on then-SEC Chair Mary Jo White to reassess the materiality framework in the context of cybersecurity disclosures. Calling the existing definitions of materiality "naïve," Langevin and Himes wrote, "materiality as it relates to cyber risk is particularly difficult to assess both because we lack sufficient data from past cyber attacks and because the effects are often not distinguishable from the many confounding variables surrounding a company's earnings."

Toward practical disclosures. Congress has thus far not enacted cybersecurity laws that would directly affect public company disclosures. In the 114th Congress, former Rep. Jim McDermott (D-Wash) introduced the Cybersecurity Systems and Risks Reporting Act (H.R. 5069), which would have invoked the Sarbanes-Oxley Act's executive certification and internal controls provisions. Senators Jack Reed (D-RI) and Susan Collins (R-Maine) also introduced the Cybersecurity Disclosure Act of 2015 (S. 2410), which would have required companies to disclose if their boards have cybersecurity expertise. Senator Reed reintroduced the bill in the 115th Congress (S. 536).

Practically speaking, however, the web of state-law data breach notification requirements such as Delaware's make disclosure compulsory, even absent laws and rules at the federal level. Some states, such as California, publish the notices that must be sent to the state attorney general if a certain number of residents are affected. Companies preparing a response to a cyber incident must be mindful of the concurrent requirements of all jurisdictions in which they do business.