New York Law Journal

NEW YORK LAW JOURNAL SPECIAL REPORT

An ALM Publication

Cybersecurity

WWW.NYLJ.COM

VOLUME 259—NO. 106

MONDAY, JUNE 4, 2018

The Challenges Of a National 72-Hour Data Breach Notification Standard

BY NICOLE FRIEDLANDER, COREY OMER AND JOHN EVANGELAKOS

Facebook CEO Mark Zuckerberg testified before Congress last month regarding Cambridge Analytica's unauthorized use of data of an estimated 87 million Facebook users to profile and target voters during the 2016 U.S. presidential election. During questioning, Senator Amy Klobuchar of Minnesota asked whether Zuckerberg would support a rule requiring Facebook to notify its users of a data breach within 72 hours, and Zuckerberg suggested that he would. Thereafter, on April 23, Senators Klobuchar and John Kennedy of Louisiana introduced the "Social Media Privacy Protection and Consumer Rights Act

NICOLE FRIEDLANDER *is special counsel,* COREY OMER *is an associate and* JOHN EVANGELAKOS *is a partner at Sullivan & Cromwell.*

of 2018" (S. 2728), which would require "covered online platforms," including public-facing websites, web applications, mobile applications, and email services, to provide notice of a data breach to affected users within 72 hours of learning that personal data about the users was inappropriately transmitted.

Amidst the patchwork of competing state laws and sector-specific federal standards, support has been growing for a preemptive federal standard for notification following a cybersecurity incident involving the exposure of personal information. Currently, notification following a breach is governed by 50 different state laws, as well as sector-specific standards such as the Gramm-Leach-Bliley Act (applicable to the financial services industry) and the Health Insurance Portability and Accountability Act (applicable to personal health care information). These laws vary widely with respect to the requirements they impose on covered entities, including the categories of compromised data and types of compromise that trigger a notice requirement, the time frame within which notice must be provided, and the information that must be included in any notice.

In some instances, state laws even contradict each other: Massachusetts, for example, prohibits describing the nature of a breach in any notice, while some other states, including North Carolina, expressly mandate that such information be included. Moreover, states have been amending their breach notification laws with a frequency that complicates the challenge of complying with them. Since the start of 2018 alone, at least 30 states have enacted or are considering bills that would amend existing laws to, among other things, expand the range of covered information and impose stricter deadlines for providing breach notification. This web of varied and changing requirements can be challenging for any entity—and particularly one in the midst of a significant cybersecurity incident—to navigate.

While there may be significant benefits to a federal standard, it is critical that any standard incorporate the practical challenges of responding to a data breach. Beyond the fact that the proposed Senate bill would introduce yet another sector-specific breach notification law rather than a law of general applicability with preemptive effect, in our experience, the provision of notice to affected persons within 72 hours of learning of a cybersecurity incident is often very challenging, if not impossible, and may create substantial confusion for consumers as well as legal and reputational risks for the company.

Steps to Providing Accurate Notice

Providing accurate notice of a cybersecurity incident typically involves multiple steps. *First*, large companies may face hundreds or more attempted cyberattacks per day. Once a potential incident is detected internally, the security team must determine its significance and escalate it to the appropriate stakeholders, and the company may need to communicate with law enforcement and regulators. This process can take days even for a company that is working around the clock with substantial resources, sophistication, and expertise. Further, in some instances, organizations only learn that they have suffered a data breach from law enforcement, which does not necessarily know or may not be in a position to share information about how or when the company was compromised or what data was exposed. In these circumstances, the company must work to try to identify the source of the compromise. This can be a challenge far beyond that of finding a needle in a haystack, and generally involves the retention of third-party cybersecurity experts who may or may not be able to identify the compromise after substantial investigation.

Second, even where a company is aware of a cybersecurity incident, assessing the breadth and depth of the compromise often requires days or weeks of forensic examination. Malicious actors may secure multiple footholds in a compromised environment, and frequently take steps to hide their digital footprints in a company's network. Thus, identifying what information hackers have accessed or exfiltrated can be a complex task even in seemingly unsophisticated breaches. This task may be further complicated where the cooperation of a vendor or third party—increasingly a vector through which breaches occur—is needed to investigate compromised servers.

Third, once a compromised dataset is identified, matching that data to the person who must be notified is often challenging. For example, a company may discover that a large set of personal data, such as driver's license or social security numbers, has been compromised. But a breach notification letter cannot be sent to a driver's license or social security number. Thus, the affected company frequently must try to match the compromised data with other records, if available, to try to identify the person associated with the data, and then identify accurate contact information for that person. This can be particularly challenging when affected persons are not the company's direct customers (for example, where

a company has data concerning family members or employees of a customer).

Finally, once the company is in a position to draft a notice, the notice must be accurate and appropriately vetted by company stakeholders. Further, when printed notices are required, the mechanical process of distributing such notices typically, on its own, takes several days, even where vendors are working on an expedited basis.

Further Risks

Beyond the practical difficulties of complying with a 72-hour notice standard, such a requirement may expose the company to legal and reputational risks. In our experience, even with the best cybersecurity teams and external advisors, companies' understanding of the nature of any significant compromise—including who and what data was affected—often changes significantly in the days after a breach is discovered. Providing customers with inaccurate or incomplete information about whether and to what extent their data has been affected can be problematic and confusing for them, potentially more so than providing late notification. The company may be inundated with questions from customers that it cannot answer, which may frustrate customers, and this process may divert substantial company resources and senior management focus at the very time those are most needed to remedy the incident and avert further customer harm.

Securities law disclosure requirements further complicate the risks to public companies of providing notice too early. To avoid running afoul of selective disclosure laws, a company may feel it necessary to issue a press release concerning a material

cybersecurity incident. Thus, if notice is required too soon, it is not only a discrete group of people who may receive inaccurate or incomplete information, but the public and the market generally. If a public company later needs to amend its notice to correct previous statements, it runs the risk of exposure to securities law claims based on inaccuracies in the prior notice. And aside from legal challenges, companies have regularly faced public criticism for providing early breach notification that later required amendments based on updated information.

Regulations

Proponents of a 72-hour notice requirement have pointed to the New York State Department of Financial Services (the NYDFS) Cybersecurity Regulation, 23 N.Y.C.R.R. 500, and the European Union's General Data Protection Regulation (the GDPR) as examples of legislation with equally demanding notice requirements, but neither regulation requires notice to affected individuals within such a short time frame. The NYDFS Cyber Regulation requires notice only to the NYDFS within 72 hours, and such notice constitutes confidential supervisory information that is protected from further disclosure. Similarly, the GDPR requires notice only to the relevant national Supervisory Authority within 72 hours, and even that notice may be provided in phases if the company is unable to provide all required information in its initial notice. By contrast, under the GDPR, notice to affected individuals must be made "without undue delay."

Fortunately, Congress is currently considering other notification standards that balance the need for prompt notice with the challenge of providing accurate notice to affected persons. The "Data Security and Breach Notification Act" (S. 2179), introduced in the Senate on Nov. 30, 2017, would require entities to notify affected individuals and the Federal Trade Commission within 30 days of discovering a breach or "as promptly as possible" if such notice is not feasible due to circumstances necessary to accurately identify affected consumers, prevent further breach, or reasonably restore the integrity of the data system. Likewise, the bipartisan "Data Acquisition and Technology Accountability and Security Act," first circulated in the House in February 2018, would require entities to notify consumers of a breach "immediately…without unreasonable delay" if, after completion of a preliminary investigation, the entity determines there is a reasonable risk the breach will result in identity theft, fraud, or economic loss. Both of these bills appear to be workable starting points for discussion of a national data breach notification standard, reflecting both the need for prompt customer notification and the practical challenges of responding to a cybersecurity incident.