Morgan Lewis

alert

advertising, consumer protection, and privacy lawflash

www.morganlewis.com

Recent SEC Guidance and Upcoming Amendments to California and Illinois Statutes Affect Data Breach Disclosure Obligations

November 16, 2011

Recognizing that business entities now conduct a majority of their operations with the assistance of electronic programs and databases, and that a significant amount of business and personal information may be stored electronically in those systems, state legislatures and financial regulators are taking steps to identify the risks inherent in such computer-driven operations. Covered companies that are registered with the SEC and that collect or electronically store their clients' and employees' personal information run the risk of experiencing an unauthorized breach of that data by hacking, inadvertent dissemination, loss or theft of portable devices containing such information, or other unauthorized disclosure. If a data breach occurs, a covered company's responsibility to disseminate information about the breach may be broadened under the SEC's recent guidance.

SEC Releases Guidance Outlining Disclosure Obligations

On October 13, the Securities and Exchange Commission (SEC) released guidance[1] relating to a covered business entity's obligations to disclose cybersecurity risks and data breach incidents within SEC registrants' already-required SEC disclosures and filings. The SEC provided this guidance in an effort to instruct business entities on what situations call for disclosure of information about potential and/or actual data security breaches in public filings, and what amount of detail should be provided.

Currently, 46 states plus the District of Columbia, Puerto Rico, and the U.S. Virgin Islands have enacted laws requiring companies to notify individuals within their jurisdiction if their personal information has been implicated in a data security breach incident. While each state's threshold requirements for notification vary, notification is typically required when information such as a person's Social Security number, driver's license number, or bank account number, in conjunction with other personal identifying information, has been or is "reasonably believed" to have been breached. While the new SEC guidance does not add any requirements to a company's state-by-state obligations to notify affected individuals in these situations, companies should consider the SEC's current position when considering whether similar disclosures about the breach must be included in SEC filings.

In the event that a covered company experiences what the SEC terms a "material cyber attack," in the

1. View the guidance online at http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

form of a data breach incident requiring notification, the SEC guidance indicates that the following factors associated with the breach may require disclosure in SEC-required filings:

- Financial disclosures regarding the remediation costs incurred or expected to be incurred by the business entity. Such costs could include the costs of credit monitoring for affected individuals, costs of preparing and disseminating the data breach notifications, and costs associated with use of notification vendors.
- Financial disclosures regarding the cost of a business entity's increased cybersecurity aimed at preventing future data breach incidents.
- Financial disclosures regarding actual or potential loss in revenue due to reputational damage stemming from the data breach incident or actual revenue loss due to the effects of the data breach.
- Legal disclosures regarding filed litigation stemming from the data breach, if the potential litigation would be material.

Additionally, if a business entity concludes that there is a risk of future cybersecurity/data breach incidents due to its systems not rigorously protecting data, the SEC guidance indicates that a business entity must disclose those facts if they make "investment in the company speculative or risky."

The SEC guidance stops short of requiring registrants to modify or enhance the notifications and disclosures that are already mandated by each state's data breach statutes, in part because it is cognizant that "detailed disclosures could compromise cybersecurity efforts—for example, by providing a 'roadmap' for those who seek to infiltrate a registrant's network security."

Nevertheless, the SEC guidance makes it clear that, in addition to compliance with state data breach notification requirements, various existing SEC requirements may necessitate additional disclosure of a data breach incident or its aftereffects in a business entity's public filings. Business entities must therefore not only follow the letter of each state's notification laws, but also consider whether and how each data breach incident should be disclosed in their regular public filings.

California and Illinois Data Breach Requirements

In other news occurring in the data breach realm, California, the original data breach statute state, and Illinois have both amended their data breach statutes.

California's amendments, which go into effect on January 1, 2012, incorporate many of the recent developments in other states. In data breach situations where more than 500 people are affected, for example, California's statute will require companies to "electronically submit a single sample" of the notification letter to the state's attorney general, excluding any personally identifiable information. The new law amends the substitute notice provisions and addresses the relationship with federal requirements for companies subject to HIPPA.

The California amendments also clarify that data breach notices to affected individuals must be written in "plain language" and include the following:

- A general description of the breach
- The name of and contact information for the reporting entity

- The types of personal information that were "or are reasonably believed" to have been part of the breach
- The date or estimated date of the breach, and the length of the breach
- Whether notification was delayed by law enforcement
- Toll-free telephone numbers and addresses of the credit reporting agencies (CRAs), only if the breach included Social Security numbers, driver's license numbers, or California ID card numbers

Illinois has also amended its data breach notification requirements, with the amendments likewise going into effect on January 1, 2012. Illinois's amendments also mainly concern the content of a data breach notification. The state will require data breach notifications to include the toll-free numbers and addresses for the CRAs and the Federal Trade Commission, as well as "statement that the individual can obtain information from these sources about fraud alerts and security freezes." Of note, the Illinois amendments specifically state that notifications to affected individuals shall not include the number of Illinois residents affected by the breach.

Implications

Companies regularly collect and store personal information from both their clients and their employees, creating a risk that this sensitive information could be inadvertently disclosed or accessed without authorization. In the case of a data breach, companies should not only be prepared to follow each state's requirements regarding notification and remediation of the breach and their contractual obligations to their customers, but also consider the implications of the breach upon their SEC filing requirements. These considerations should be included in a data breach incident response plan that the company follows if a breach occurs.

If you have any questions about the issues discussed in this LawFlash or would like to discuss implementation of a data breach incident response plan, please contact any of the following Morgan Lewis attorneys:

Washington, D.C.
Ron N. Dreben 202.739.5213 rdreben@morganlewis.com

Chicago
Kenneth M. Kliebard 312.324.1774 kkliebard@morganlewis.com

Philadelphia
Gregory T. Parks 215.963.5170 gparks@morganlewis.com
K. Catherine Roney 215.963.5722 kroney@morganlewis.com

San Francisco
Rochelle D. Alpert 415.442.1326 ralpert@morganlewis.com
W. Reece Hirsch 415.442.1422 rhirsch@morganlewis.com
Carla B. Oakley 415.442.1301 coakley@morganlewis.com

About Morgan Lewis's Advertising, Consumer Protection, and Privacy Practice
Morgan Lewis's Advertising, Consumer Protection, and Privacy Practice consists of more than 40 lawyers and legal professionals serving clients in a broad range of industries. Our team has experience

litigating federal and state false advertising and unfair competition claims brought by competitors, federal and state government agencies, and consumer classes. We regularly advise on U.S. and global advertising and marketing regulations and clearance requirements, and analyze contests, sweepstakes, and promotions in social media, the Internet, and more traditional media to ensure compliance with the myriad rules and regulations involved. Our comprehensive array of privacy and data security experience includes advising clients on compliance with U.S. (federal and state) and EU data security requirements. We also draft and negotiate a full range of agreements in connection with innovative marketing and promotional activities. For more information about the Advertising, Consumer Protection, and Privacy Practice, please visit us online at www.morganlewis.com/privacy.

About Morgan, Lewis & Bockius LLP

With 22 offices in the United States, Europe, and Asia, Morgan Lewis provides comprehensive transactional, litigation, labor and employment, regulatory, and intellectual property legal services to clients of all sizes—from global Fortune 100 companies to just-conceived startups—across all major industries. Our international team of attorneys, patent agents, employee benefits advisors, regulatory scientists, and other specialists—nearly 3,000 professionals total—serves clients from locations in Beijing, Boston, Brussels, Chicago, Dallas, Frankfurt, Harrisburg, Houston, Irvine, London, Los Angeles, Miami, New York, Palo Alto, Paris, Philadelphia, Pittsburgh, Princeton, San Francisco, Tokyo, Washington, D.C., and Wilmington. For more information about Morgan Lewis or its practices, please visit us online at www.morganlewis.com.