CLIENT ALERT: Disclosing Cybersecurity Risks and Incidents and Concomitant Financial, Legal and Reputational Consequences

CLIENT ALERT | 02.28.2018
Spencer G. Feldman

PROFESSIONALS

Spencer G. Feldman

PRACTICE AREAS

Corporate/Securities Law

On February 21, 2018, the SEC published interpretive guidance to assist public companies in preparing disclosures about cybersecurity risks and incidents. Below is a summary outlining this new disclosure category which impacts all public companies, regardless of their size, and applies to all prospectuses and periodic reports filed with the SEC.

The SEC has indicated that it, and its staff through the filing review process, will monitor cybersecurity disclosures carefully, beginning with this annual report season.

Summary of the SEC's Cybersecurity Disclosure Guidance

Why Disclose:

Public companies need to:

- take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion;
- have disclosure controls and procedures in which directors, officers and other responsible persons are informed about the cybersecurity risks and incidents that are faced or will likely be faced; and
- adopt policies and procedures to guard against directors, officers and other corporate insiders trading on material nonpublic information about a cyber-event prior to its disclosure to the public.

Where to Disclose:

Existing disclosure requirements of Regulation S-K impose an obligation to provide timely and ongoing disclosure of material cybersecurity risks and incidents in the following SEC filings:

Annual Reports on Form 10-K

- Business and Operations (Item 101);
- Risk Factors (Item 503);
- Legal Proceedings (Item 103);
- Management's Discussion and Analysis of Financial Condition and Results of Operations ("MD&A") (Item 303);
- Financial Statements (Regulation S-X);
- Disclosure Controls and Procedures (Item 307); and
- Corporate Governance (Item 407).

Quarterly Reports on Form 10-Q

- Financial Statements;
- MD&A; and
- Updated Risk Factors.

Registration Statements

- Cybersecurity-related disclosure obligations run throughout registration statements in that all material facts are required to be stated therein or necessary to make the statements therein not misleading.

Current Reports on Form 8-K

- Regulation FD Disclosure (Item 7.01); and
- Other Events (Item 8.01).

Whether to Disclose:

In determining one's disclosure obligation, a company must weigh the potential materiality of any identified risk, and the importance of any compromised information and the impact of any incident on the company's operations. Materiality is not necessarily a quantifiable measure as it includes harm to a company's reputation and customer and vendor relationships, and the possibility of litigation or regulatory investigations by government authorities.

"Roadmap" Risk Should be Minimized – Companies are not expected to disclose specific, technical information about their cybersecurity systems (e.g., firewalls and intrusion detection software) or potential system vulnerabilities in such detail as would make such systems, networks and devices more susceptible to a cyber-attack from a would-be hacker.

When to Disclose:

When a company has become aware of a material cybersecurity incident or risk, a disclosure must be *timely*, which would be, for example, (i) prior to the offer and sale of securities and (ii) to prevent directors, officers and corporate insiders from trading a company's securities until investors have been appropriately informed about the risk or incident. Even if there is no specific Form 8-K reporting item for cybersecurity incidents, it is recommended that a company report an incident promptly under Form 8-K Item 7.01 or 8.01.

Can't Wait for Full Investigation – An initial disclosure of a material cybersecurity incident is required to be made when discovered. An ongoing internal or external investigation, which can take weeks if not months, is *not* an acceptable excuse to postpone disclosure. Companies should update their disclosure during the process of investigating the cybersecurity incident.

What to Disclose:

Without using unspecific boilerplate language or generic cybersecurity-related disclosure, cybersecurity risk factors should address:

Risk Factors

- occurrence of previous or ongoing cybersecurity incidents (such as cyber-attacks using stolen access credentials, malware, ransomware, phishing, structured query language injection attacks and distributed denial-of-service attacks), and their severity and frequency;
- probability of the occurrence and potential magnitude of such incidents;
- adequacy of preventative actions taken to reduce cybersecurity risks and associated costs;
- aspects of the company's business that give rise to particular types of cybersecurity risks, including the risks that arise in connection with acquisitions, and the potential costs and consequences of such risks;
- costs associated with maintaining cybersecurity protections (e.g., insurance coverage and payments to computer consulting firms);
- potential for reputational harm;
- existing and pending laws and regulations relating to cybersecurity applicable to the company; and
- litigation, regulatory investigations and remediation costs of cybersecurity incidents.

MD&A

Management's discussion of its financial condition, changes in financial condition and results of operations should address:

- cost of ongoing cybersecurity efforts;
- costs and other consequences of cybersecurity incidents; and
- risks of potential cybersecurity incidents.

Costs, in this context, should be construed broadly beyond a temporary shutdown of a business to include:

- loss or theft of intellectual property and other valuable data;
- implementing preventative measures;
- maintaining insurance;
- responding to litigation and regulatory investigations;
- preparing for and complying with proposed or current legislation;
- engaging in remediation efforts;
- addressing harm to reputation; and
- loss of competitive advantage that may result.

Business

Appropriate disclosure in the business section of SEC filings is required if cybersecurity incidents or risks materially affect a company's mode of conducting business or its products, services, relationships with customers or suppliers, or competitive conditions. This applies essentially to any company that relies on information, and not only e-commerce and other technology companies.

Legal Proceedings

Legal proceedings that relate to cybersecurity issues, such as litigation by customers against a company that has experienced an incident involving theft of customer information, must be properly described in this section like all other types of litigation. This disclosure is still subject to the applicable litigation disclosure thresholds set forth in Regulation S-K.

Financial Statements

Financial impacts of a cybersecurity incident that may need to be incorporated into a company's financial statements and related notes include:

- expenses related to an investigation, breach notification, remediation and litigation, plus legal and other professional services;
- loss of revenue or providing customers with incentives;
- claims related to warranties, breach of contract, product recall/replacement, indemnification of counterparties and insurance premium increases; and
- diminished future cash flows, impairment of intellectual, intangible or other assets, and recognition of liabilities.

Board Risk Oversight

In a company's description of how its board administers its risk oversight function, additional disclosure should be added to include the nature of the board's role in overseeing the management of cybersecurity risks.

How to Verify Disclosure:

The SEC encourages all companies to adopt comprehensive cybersecurity policies and procedures and assess their compliance regularly.

Companies must maintain disclosure controls and procedures, and management must evaluate their effectiveness, to ensure that relevant information about cybersecurity risks and incidents is processed and reported to the appropriate personnel (including "up the ladder" from an IT manager or Chief Information Officer to and through the full board of directors) to:

- enable senior management to make disclosure decisions and certifications; and
- facilitate policies and procedures to prohibit directors, officers and other insiders from trading on the basis of material nonpublic information about cybersecurity incidents.

Reminder to PEOs and PFOs. Certifications in periodic SEC reports of a company's principal executive officer and principal financial officer must take into account the adequacy of controls and procedures for identifying cybersecurity risks and incidents and for assessing and analyzing their impact.

What Else Does SEC Advise on Disclosure:

Information about cybersecurity risks and incidents, including vulnerabilities and breaches, may be material nonpublic information; it is illegal for directors, officers and other insiders to trade the company's securities in breach of their duty of trust and confidence in possession of that information.

The SEC encourages all companies to consider how their codes of ethics and insider trading policies take into account and prevent trading on the basis of material nonpublic information related to cybersecurity risks and incidents and, in particular, during the period following an incident and prior to the dissemination of disclosure. This issue may be more complicated while companies are investigating and accessing significant cybersecurity incidents, and determining the underlying facts, ramifications and materiality of these incidents.

Companies and persons acting on their behalf must be careful to not selectively disclose material nonpublic information regarding cybersecurity risks and incidents to Regulation FD enumerated persons before disclosing that same information to the public.

For more information regarding the SEC's cybersecurity interpretive guidance and how to properly disclose cybersecurity risks and incidents in your SEC filings, please contact the Olshan attorney with whom you regularly work or Spencer G. Feldman of this firm.

advertising.