Brothers Smith LLP
Attorneys at Law

Featured News

ALERT

New SEC Rules Regarding Mandatory Disclosures Concerning Privacy and Cybersecurity Attacks

In 2018, the Securities Exchange Commission ("SEC") stated that companies should consider the materiality of cybersecurity risks and incidents when preparing their filings.[1] On July 26th, the SEC adopted rules requiring most public companies to disclose material cybersecurity incidents that they experience, the likely material effects of the cyber incidents, and annual disclosures of cybersecurity risk management, governance, strategy and experience. The new rules are intended to result in consistent and decision-useful disclosures to assist investors in evaluating investments as they may relate to cybersecurity risks and strategic management of those risks. However, it is clear that the new rules will also result in increased mandatory vigilance and complexity in the identification and disclosure of material cybersecurity management, reporting, and likely adverse impacts to reporting companies.

Many businesses inform their shareholders and clients of the occurrence of cyber breaches and the implementation of measures that they take in order to prevent or repair such breaches, attacks and leaks. However, these disclosures are now mandatory on at least an annual basis for companies that are subject to reporting requirements of the Securities Exchange Act of 1934. For example, when filing the annual Form 10-K, registrants are now required to describe their processes for assessing, identifying, and managing material risks from cybersecurity threats as well as current and likely material impacts of risks from cyber incidents. Management's role and expertise regarding the positions or committees who are responsible for assessing and managing such cyber risks must be identified. Even the board of directors' oversight of risks from cyber threats are required be disclosed.

Additionally, material cybersecurity incidents will be required disclosures in the new Form 8-K. A material cybersecurity incident includes the cyber incident's nature, scope, timing, and material and likely impact that it will have on costs to remediate the incident, potential loss of customers, revenue impacts, etc. A reporting company must determine if a cybersecurity incident is material "without unreasonable delay after the discovery of the incident."[2] With few exceptions, if a reporting company determines that a cybersecurity

incident is material, the company must disclose the incident within four (4) business days from the date of determination, including forward-thinking material impacts that the cybersecurity incident may have.

Specifically, cybersecurity incidents that require disclosure include "an unauthorized occurrence, or a series of related occurrences, on or conducted through a registrant's information systems that jeopardizes the confidentiality, integrity or availability of a registrant's information systems or any information residing therein." [3] "Information systems" are broadly defined and refer to those owned by or used by a company, which include those utilized by a company that are owned by third parties.[4] Further, while any one of the cyber incidents in a series of related occurrences may not in and of itself have a material impact, a series of related events do cause such collective occurrences to constitute a material impact under this new rule. Examples of this include multiple, smaller occurrences by the same entity or a series of occurrences exploiting the same vulnerability. These rules affect domestic registrants as well as foreign private issuers.

With the exception of smaller reporting companies, all registrants will be required to begin complying on the later to occur of ninety (90) days after the date of publication in the Federal Register or December 18, 2023. Smaller reporting companies will have an additional 180 days.

In light of the foregoing, registrants should take immediate steps in order to ensure that their cybersecurity processes are functioning properly, up to date, and capable of the detection of unauthorized occurrences as well as the determination of which occurrences are material in order to eliminate unnecessary delays of materiality determinations and resulting required disclosures within the four (4) business-day window.

If you have any questions or would like any further guidance in regard to your privacy procedures, please feel free to contact our office.

---

1. Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Release No. 33-10459 (Feb. 21, 2018) [83 FR 8166 (Feb. 26, 2018)], available at https://www.sec.gov/rules/interp/2018/33-10459.pdf.
2. Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Release No. 33-11216 (July 26, 2023) ("Adopting Release") at 37-38.
3. 46 CFR 64.2011(b)(1)
4. *Id*.

Author

Leopold W. Lueddemann
T 925.944.9700
llueddemann@brotherssmithlaw.com

Learn More

Stay Connected

Email Us

2033 North Main Street, Suite 720
Walnut Creek, California 94596
T 925.944.9700 F 925.944.9701

www.brotherssmithlaw.com