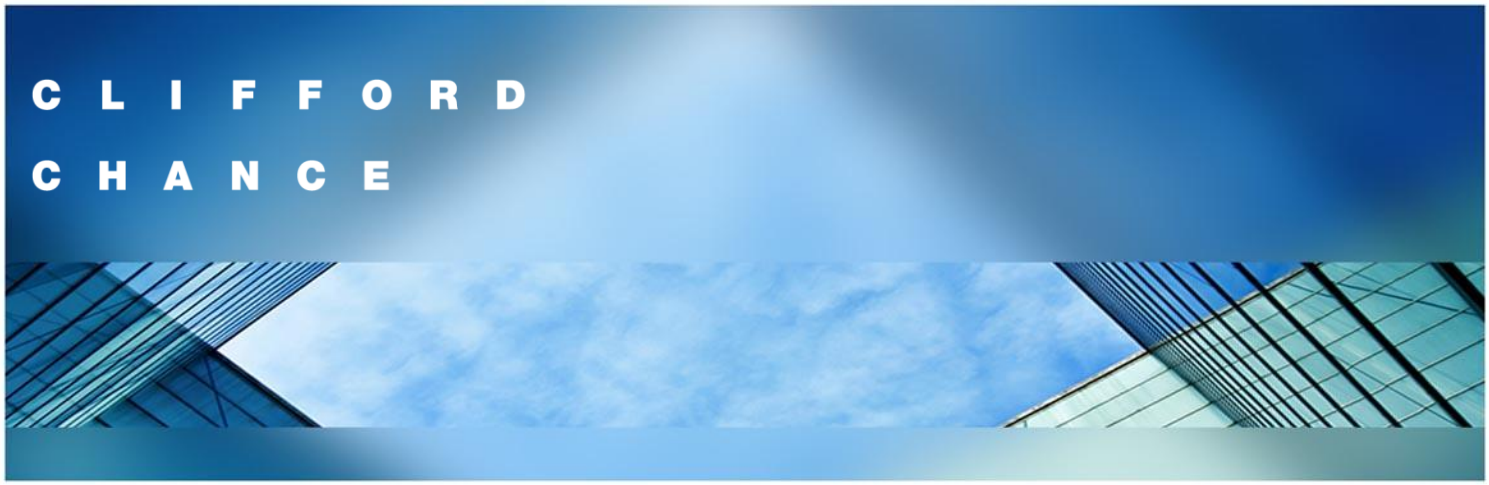

SEC PROPOSES EXPANSIVE NEW CYBERSECURITY DISCLOSURE REGULATIONS FOR PUBLIC COMPANIES

On March 9, 2022, the U.S. Securities and Exchange Commission proposed rules that would require public companies to report material cybersecurity incidents within four business days and make periodic disclosures regarding their cybersecurity risk management, strategy, and governance. If enacted in their current form, these rules would impose substantial new disclosure requirements on many issuers.

In recent years, cybersecurity attacks on public companies have increased in both number and severity, posing a threat to issuers themselves, as well as investors and other market participants. Under the Securities Exchange Act of 1934, public companies with more than $10 million in assets whose securities are held by 2,000 or more record holders or 500 or more record holders that are not accredited investors ("issuers") must file periodic public reports. In addition to annual and quarterly reports, domestic issuers must also file current reports on Form 8-K to promptly inform investors and the public of major company events. Although current U.S. Securities and Exchange Commission ("SEC") guidance advises issuers to provide timely disclosure about material cybersecurity risks and incidents in their periodic and annual reports, there are currently no uniform regulations on when, where, and how cybersecurity disclosures should be provided. As a result, the SEC has indicated a growing concern that cybersecurity incidents are often underreported, and that when reporting occurs, it is often untimely and inconsistent. Thus, the SEC concluded that mandatory prescriptive reporting and disclosure requirements are necessary. In their current form, the rules would apply to all issuers, including foreign private issuers and business development companies.

CYBERSECURITY INCIDENT REPORTING

The proposed rules would require issuers to report material cybersecurity incidents in a current report on Form 8-K within four business days of determining the incident has occurred. Issuers would also be required to supplement their

disclosures in subsequent periodic reports as more information about the incident becomes available.

What types of incidents do I have to report?

Issuers would only need to report "material" cybersecurity incidents. An incident would be considered material if "there is a substantial likelihood that a reasonable shareholder would consider it important" in making an investment decision, or it would have "significantly altered the 'total mix' of information made available." The SEC emphasizes that this materiality determination should not be a "mechanical exercise," and rather should be a "well-reasoned, objective approach," considering all relevant facts and circumstances, including both quantitative and qualitative factors.

Some examples of cybersecurity incidents that would need to be reported if deemed "material" include:

- An unauthorized party stealing sensitive business information, personally identifiable information, intellectual property, or information that would cause loss or liability for the issuer;
- An unauthorized incident that has compromised the confidentiality, integrity, or availability of an information data, system, or network;
- An unauthorized incident where a malicious counterparty demands payment to restore stolen or altered company data

The proposed rules would also require issuers to disclose any previously undisclosed cybersecurity incidents that the issuer deemed to be immaterial when considered individually, but that in the aggregate have become material. Rather than a Form 8-K, these disclosures would be made in the periodic report for the period in which the issuer has determined the cybersecurity incidents have become collectively material.

What should a report include?

Issuers would be required to provide the following information, to the extent it is known at the time of the filing:

- when the incident was discovered and whether it is ongoing;
- a brief description of the nature and scope of the incident;
- whether any data was stolen, altered, accessed, or used for any other unauthorized purpose;
- the effect of the incident on the issuer's operations; and
- whether the issuer has remediated or is currently remediating the incident.

In providing the above information, issuers would not be expected to disclose technical information regarding how they plan to respond to incidents or details on their cybersecurity systems, networks, and devices that would negatively impact issuers' remediation efforts (e.g., if doing so would provide information that attackers could use for subsequent attacks).

When would I need to report?

Issuers would be required to report material cybersecurity incidents within four business days. This four-business-days reporting window would begin when the issuer determines the cybersecurity incident is material, which the SEC recognized may be later than the date the issuer realizes the incident has occurred. Issuers would be expected to make their materiality determination "as soon as reasonably practicable after the discovery of the incident."

For context, this four-business-days reporting requirement is slightly more generous than other recent cybersecurity incident reporting regulations. The New York State Department of Financial Services (NYDFS) Cybersecurity Regulation and EU General Data Protection Regulation (GDPR) both require notification within 72 hours. Federal banking regulators recently issued a final rule requiring notification within 36 hours,[1] and the SEC's proposed rule last month for registered investment advisers and funds would require notification within 48 hours.[2] That being said, many U.S. state incident reporting requirements provide for a longer time frame and against more subjective criteria (e.g., "without unreasonable delay"). Conceivably, the four-business-days reporting requirement for issuers could impact what states consider to be a reasonable timeframe under their laws as well.

An ongoing internal or external investigation would not be a valid reason to delay reporting. Even in circumstances where a state law may allow for delay in reporting due to a criminal investigation, reporting on Form 8-K would still be required. The SEC acknowledged that delayed reporting can be beneficial for some investigations, but in its proposed rule the SEC stated that it believes the importance of timely disclosure to investors outweighs any such benefit.

Are any follow-up reports required?

In addition to the initial reporting requirement, the proposed regulations would also require issuers to provide information regarding material cybersecurity incidents in periodic disclosures as well. The rules would require issuers to provide information on any updates, material changes, or additions to their Form 8-K cybersecurity incident disclosures with their Form 10-Q or Form 10-K reports. For example, issuers would be required to provide information on how they have remediated cybersecurity incidents or how incidents have affected their operations, which likely would not have been available at the time of the initial reporting.

Will there be consequences for untimely or incorrect reporting?

Although the rules stress the importance of timely reporting, an untimely filing will not, by itself, void an issuer's eligibility to file simplified security registration statements under Form S-3 or Form SF-3.

Additionally, the SEC plans to add the material cybersecurity incident reporting section as one of the Form 8-K items eligible for a limited safe harbor exemption

---

1 For more on this rule, see our briefing here: https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2021/11/US-federal-banking-agencies-issue-rule-requiring-banks-to-notify-regulators-of-cyber-incidents-within-36-hours.pdf

2 For more on these proposed rules, see our briefing here: https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2022/02/SEC%20Proposes%20Substantial%20New%20Cybersecurity%20Regulations%20For%20Registered%20Investment%20Advisers%20And%20Funds.pdf

from liability under Section 10(b) or Rule 10b-5 of the Exchange Act, which make it illegal to make materially misleading statements, omissions, or misrepresentations in disclosures, among other things. This limited safe harbor allows issuers to avoid liability from penalties under Section 10(b) and Rule 10b-5 for failure to timely file a Form 8-K, but it does not shield them from liability for misstatements in filed reports or from liability that may arise from failing to timely disclose under other securities laws. The safe harbor is also limited in duration, expiring upon the due date of the issuer's next periodic report for the period in which the Form 8-K should have been filed. The SEC has previously determined that such a safe harbor is appropriate when the triggering event for the Form 8-K is based on a rapid materiality determination. Since the proposed rules require materiality to be decided as soon as reasonably practicable, issuers may need to make a rapid materiality determination when complying with the rules.

CYBERSECURITY RISK MANAGEMENT, STRATEGY, AND GOVERNANCE DISCLOSURE REQUIREMENTS

The proposed regulations would also amend Regulation S-K to require issuers to make disclosures regarding their policies and procedures regarding cybersecurity risk management, strategy, and governance.

With respect to cybersecurity risk management and strategy, the rules would require disclosure on eight different subtopics, including:

- whether the issuer has a cybersecurity risk assessment program (and if so, a description of such program);
- whether the issuer has business continuity, contingency, and recovery plans in the event of a cybersecurity incident;
- whether the issuer has policies and procedures to oversee and identify cybersecurity risks associated with using a third-party service provider; and
- whether cybersecurity risks are considered as part of the issuer’s business strategy, financial planning, and capital allocation (and if so, how).

With respect to governance-related disclosures, an issuer would be required to disclose details on the board's oversight of cybersecurity risks, a description of management's role in assessing and managing cybersecurity risks, the relevant expertise of such management, and management's role in implementing cybersecurity policies, procedures, and strategies. This would include, among several other items, reporting specific details such as how frequently the board discusses cybersecurity risks, the process by which the board is informed of cybersecurity risks, and whether an issuer has a designated chief information security officer—and if so, where that person falls in the organizational chart.

The proposed regulations would also amend Regulation S-K to require issuers to disclose the cybersecurity expertise of members of their boards of directors. If any board member has cybersecurity experience, the issuer would be required to disclose that individual's name and provide any detail necessary to fully describe that expertise. As noted in the proposed rule, the SEC intends for this requirement to give investors information they may need as they consider their

investment in a particular issuer and consider how to vote in board elections. Issuers would be required to provide this information in both their annual 10-K report and their proxy or information statements.

APPLICATION TO FOREIGN PRIVATE ISSUERS

The proposed regulations would also apply to foreign private issuers ("FPIs") that are subject to certain disclosure requirements under the Securities Act of 1934. The proposed rules would add material cybersecurity incidents as an event that can trigger a Form 6-K report. FPIs would also be required to report previously undisclosed immaterial incidents that in the aggregate have become material and supplemental information and updates regarding previously reported incidents in annual Form 20-F reports. Additionally, FPIs would have to disclose information regarding their cybersecurity risk management, strategy, and governance, as well as their boards' cybersecurity expertise in Form 20-F reports as well. However, unlike issuers, FPIs are not required to file proxy or information statements, and therefore would only be required to disclose their boards' expertise in their annual reports.

TAKEAWAYS

If enacted, these rules would impose significant new disclosure burdens on issuers, and robust industry comment is expected. In her dissenting statement, Commissioner Hester M. Peirce expressed her fear that these regulations would cast the SEC as the "nation's cybersecurity command center," a role that Congress did not give it, and "represent an unprecedented micromanagement by the Commission of the composition and functioning of both the boards of directors and management of public companies."

Additionally, as Commissioner Peirce acknowledged, although these regulations are framed as disclosure requirements, it is likely they will have the practical effect of impacting public companies' policies and procedures involving cybersecurity risk management, rather than just simply regulating disclosure practices. For example, Peirce cites the Sarbanes Oxley Act's requirement to disclose audit committee financial expertise, which has resulted in most companies treating having finance experts as audit committee members as a requirement. Issuers may similarly see these disclosure requirements as a new checklist by which they will be judged against their competitors on how they are managing cybersecurity risks.

Although these regulations are only proposals at this time, issuers can start taking steps now to ensure future compliance. These measures include taking stock of existing cybersecurity policies and procedures, including reporting and disclosure practices and escalation procedures to senior management and the board regarding cybersecurity risks. Issuers would also be well-advised to ensure they have sufficient cybersecurity expertise at the senior management and board level. Issuers are also encouraged to conduct risk assessments, if not already doing so, to identify and mitigate any vulnerabilities. Business development companies and their managers should also consider any interplay between this new proposal and rules proposed by the SEC last month regarding Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies.

Public comment will remain open on these proposed regulations until May 9, 2022, or 30 days from when they are published in the Federal Register, whichever period is longer.

Clifford Chance has published a number of reports to help financial services firms and other companies protect themselves from cyber attacks and comply with international reporting requirements. For more information, see our Report on What Cyber Regulators Are Saying Around the World as well as our Ransomware Playbook.

CLIFFORD
CHANCE

CONTACTS

Daniel Silver
Partner

T +1 212 878 4919
E daniel.silver
@cliffordchance.com

Jeff Berman
Partner

T +1 212 878 3460
E jeffrey.berman
@cliffordchance.com

Cliff Cone
Partner

T +1 212 878 3180
E clifford.cone
@cliffordchance.com

Andrew Epstein
Partner

T +1 212 878 8332
E andrew.epstein
@cliffordchance.com

Megan Gordon
Partner

T +1 202 912 5021
E megan.gordon
@cliffordchance.com

Jefferey LeMaster
Partner

T +1 212 878 3206
E jefferey.lemaster
@cliffordchance.com

Jason Myers
Partner

T +1 212 878 8324
E jason.myers
@cliffordchance.com

David Adams
Associate

T +1 202 912 5067
E davidg.adams
@cliffordchance.com

Benjamin Berringer
Associate

T +1 212 878 3372
E benjamin.berringer
@cliffordchance.com

Brian Yin
Associate

T +1 212 878 4980
E brian.yin
@cliffordchance.com

Rebecca Hoskins
Professional Support Lawyer

T +1 212 878 3118
E rebecca.hoskins
@cliffordchance.com

Hank Michael
Strategic Advisory Lawyer

T +1 212 878 8225
E hank.michael
@cliffordchance.com

Shannon O'Brien
Law Clerk

T +1 212 880 5709
E shannon.obrien
@cliffordchance.com