

New SEC-Proposed Rules Emphasizing Cybersecurity Disclosures and Governance

March 17, 2022

As we indicated in past advisories, the U.S. Securities and Exchange Commission (the “SEC”) announced on June 11, 2021 that it would be focusing on cybersecurity disclosures made by public companies as part of its regulatory agenda. On March 9, 2022, the SEC announced its much anticipated proposals to mandate cybersecurity disclosures by public issuers.

The timing of the proposals coincides with Russia’s ongoing invasion into Ukraine, which many regard as a time of acute cyber risk for U.S. and other Western corporations and governments.

These proposals were the third set of rulemaking proposals by the SEC in 2022 to have a heavy emphasis on cybersecurity. In January 2022, the SEC proposed rules related to expanding Regulation Systems Compliance and Integrity (SCI) to certain government securities trading platforms. In February, [the SEC proposed](#) new obligations for registered investment advisers and funds with respect to cybersecurity, and in March, [the SEC proposed](#) new disclosure rules for public companies. We discuss the second and third proposals herein.

I. The Investment Advisers Proposed Rules

On February 9, 2022, the SEC proposed new rules addressing cybersecurity risk management under the Investment Advisers Act of 1940 (the “Advisers Act”) and the Investment Company Act of 1940 (the “1940 Act”).

These rules will apply to investment advisers that are registered or required to be registered with the SEC and registered investment companies and closed-end companies that elect to be treated as business development companies under the 1940 Act, and, in short, will require advisers and registered funds to:

- i. adopt and implement written policies and procedures, including specific enumerated elements, reasonably designed to address cybersecurity risks.
 - ii. report certain cybersecurity incidents to the SEC on new Form ADV-C within 48 hours, including on behalf of any registered funds or private funds that experience such incidents. Under proposed Rule 204-6 of the Advisers Act, advisers will be required to report significant cybersecurity incidents to the SEC on new Form ADV-C, including on behalf of any registered funds and private funds that experience such incidents. The reports will have to be made promptly but in no event later than 48 hours after having a reasonable basis to conclude that a “significant adviser cybersecurity incident” or “significant fund cybersecurity incident” has occurred or is occurring. The new Form ADV-C will gather information regarding the nature and scope of the incident, whether customers or law enforcement were notified, and whether the incident is covered under a cybersecurity insurance policy.
 - iii. disclose cybersecurity risks and incidents in their disclosure documents.
-

- iv. maintain for five years copies of cybersecurity policies, reports of annual reviews, Form ADV-C filings, incident records, and risk assessments.

Although these rules apply only to registered funds and advisers that are registered or required to be registered with the SEC, private funds, non-U.S. investment funds and other investment vehicles managed by such advisers will be indirectly impacted by the implementation of the compliance, reporting and disclosure requirements being applied to their advisers.

These proposed rules are open for public comment until at least April 9, 2022.

II. The Public Issuers Proposed Rules

Form 8-K and 6-K Requirements

On March 9, 2022, the SEC proposed new cybersecurity disclosure rules for public issuers. If adopted, the new rules will impose substantial new reporting obligations with respect to material cybersecurity incidents for both domestic and foreign private issuers subject to reporting requirements under the Securities Exchange Act of 1934 (the “1934 Act”).

One of the most significant proposals is the amendment of Form 8-K to add Item 1.05, which will require U.S. issuers to disclose information about a cybersecurity incident within four business days after an issuer determines that it has experienced a material cybersecurity incident.

In some cases, the date of the issuer’s *materiality determination* may coincide with the date of *discovery* of an incident, but in other cases the materiality determination will come after the discovery date. If the SEC indeed adopts, as proposed, the date of the materiality determination as the Form 8-K reporting trigger the SEC says it expects issuers to be diligent in making a materiality determination in as prompt a manner as feasible.

The materiality of cybersecurity risks or incidents depends upon their nature, extent, and potential magnitude, particularly as they relate to any compromised information or the business and scope of company operations. The materiality of cybersecurity risks and incidents also depends on the range of harm that such incidents could cause. This includes harm to a company’s reputation, financial performance, and customer and vendor relationships, as well as the possibility of litigation or regulatory investigations or actions, including regulatory actions by state and federal governmental authorities and non-U.S. authorities.

Matters to report on the 8-K will include:

- when the cybersecurity 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 cybersecurity incident on the issuer’s operations; and
- whether the issuer has remediated or is currently remediating the cybersecurity incident.

Under the proposal, foreign private issuers not subject to reporting on Form 8-K will instead be required to furnish a Form 6-K to report these cybersecurity incidents. Form 6-K General Instruction B will be amended to include “cybersecurity incidents” as a potential reporting event. Similar to other reportable events under Form 6-K, an issuer will only have to provide the disclosure if it is material *and* it is required to disclose such information elsewhere (e.g., in its home country).

Failure to file a timely Form 8-K or 6-K will not lead to the loss of eligibility to offer securities on Form S-3 or Form F-3, nor will such a failure be deemed an automatic violation of the antifraud provisions of Rule 10b-5. However, filing failures can eventually result in enforcement proceedings and a finding that an issuer had inadequate controls and procedures.

Form 10-Q Guidance

Proposed Item 106(d)(1) of Regulation S-K will require issuers to disclose any material changes, additions, or updates to information required to be disclosed pursuant to Item 1.05 of Form 8-K in the company's quarterly report on Form 10-Q or annual report on Form 10-K for the period in which the material change, addition, or update occurred. This includes updates on previously reported cybersecurity incidents.

This new item is in line with what we discussed in the past – public companies must continuously make sure their disclosures are accurate (e.g., when issuers become aware of additional material information about the scope of the incident, the handling of it and whether any data was stolen or altered), and the quarterly and annual reports provide this opportunity.

Foreign private issuers are not required to file quarterly reports. However, with respect to incident disclosure, when a foreign private issuer has previously reported an incident on Form 6-K, the proposed amendments will require an update regarding such incidents, consistent with proposed Item 106(d)(1) of Regulation S-K, on the annual report Form 20-F.

Proposed Item 106(d)(2) will also require disclosure when a series of previously undisclosed individually *immaterial* cybersecurity incidents become material in the *aggregate*.

Additional 10-K Disclosure

The proposed rules amend Form 10-K to require disclosure regarding cybersecurity risk management, strategy, and governance, as specified in Items 106(b) and 106(c) of Regulation S-K.

Proposed Item 106(b) will require issuers to disclose their policies and procedures to identify and manage cybersecurity risks and threats, including: operational risk; intellectual property theft; fraud; extortion; harm to employees or customers; violation of privacy laws and other litigation and legal risk; and reputational risk.

In addition, proposed Item 106(c) will require disclosure of an issuer's cybersecurity governance, including the board's oversight of cybersecurity risks and a description of management's role in assessing and managing cybersecurity risks, any relevant cyber expertise on the board of directors, and management's role in implementing the registrant's cybersecurity policies, procedures, and strategies.

Additional 20-F Disclosure

The proposal will amend Form 20-F to require a foreign private issuer to include in its annual report on Form 20-F disclosure similar to that required for U.S. issuers. This will be under new Item 16J. As mentioned, the proposal will amend Form 20-F to require foreign private issuers to disclose on an annual basis information regarding any previously undisclosed material cybersecurity incidents that have occurred during the reporting year, including a series of previously undisclosed individually immaterial cybersecurity incidents that has become material in the aggregate.

40-F Disclosure

Canadian foreign private issuers reporting under the Multijurisdictional Disclosure System (MJDS) and filing 40-Fs are excluded from the scope of the proposal and are not subject to any of the additional cybersecurity disclosure requirements. The SEC is specifically requesting comments on this matter.

Board Expertise Disclosure

The proposal will amend Item 407 of Regulation S-K by requiring disclosure in annual reports and proxy statements about the cybersecurity expertise of members of the board of directors. If any member of the board has cybersecurity expertise, the issuer will have to disclose the names of such directors, and provide such detail as necessary to fully describe the nature of the expertise.

Foreign private issuers are not subject to SEC rules for proxy filings and thus, would only be required to include this disclosure in their annual report.

Proposed Item 407(j) does not define what constitutes “cybersecurity expertise.” However, it includes a non-exclusive list of criteria that an issuer should consider in reaching a determination on whether a director has expertise in cybersecurity. In order to alleviate liability concerns, proposed Item 407(j)(2) will state that a person who is determined to have expertise in cybersecurity will not be deemed an expert for any purpose, including for purposes of Section 11 liability, as a result of being designated or identified as a director with expertise in cybersecurity matters.

Inline XBRL

Issuers will be required to tag the information specified in the proposal using Inline XBRL. These SEC’s proposed rules are open for public comment until at least May 9, 2022.

III. Practical Considerations

The disclosure requirements basically codify the previous guidance from the SEC, notably in its [2018 Commission Statement and Guidance on Public Company Cybersecurity Disclosures](#). It does so for both U.S. issuers and foreign private issuers subject to the 1934 Act, with the main difference being that foreign private issuers do not necessarily have to reassess the previously made disclosure every quarter. The new rules stress the importance of having proper internal controls so that issuers can determine materiality of cybersecurity incidents and report material events promptly and consistently. An extra layer in the rules is the requirement to disclose Board cybersecurity expertise, as applicable.

These new rules are not intended to suggest that issuers and investment advisers should make detailed disclosures of confidential information that could compromise their cybersecurity efforts – for example, by providing a “roadmap” for those who seek to penetrate a company’s security protections. However, these proposals send a message that the SEC is serious about issuers and investment advisers (i) having robust cybersecurity incident response plans and protocols, (ii) ensuring that boards and management play a governance role in cybersecurity risk assessment and incident response, and (iii) reporting material cybersecurity incidents.

* * *

Carter Ledyard & Milburn LLP uses Client Advisories to inform clients and other interested parties of noteworthy issues, decisions and legislation which may affect them or their businesses. A Client Advisory does not constitute legal advice or an opinion. This document was not intended or written to be used, and cannot be used, for the purpose of (i) avoiding penalties under the Internal Revenue Code or (ii) promoting, marketing or recommending to another party any transaction or matter addressed herein. © 2022 Carter Ledyard & Milburn LLP.

related professionals

Guy Ben-Ami / Partner

D 212-238-8658

benami@clm.com