July 2023

Follow @Paul_Hastings

Public Company Update

The SEC Adopts Cybersecurity Disclosure Regime for Public Companies

By Sean Donahue, Jeremy Berkowitz, Brad Bondi, Aaron Charfoos, Ken Herzinger, and Spencer Young

On July 26, 2023, the U.S. Securities and Exchange Commission (the "SEC") adopted enhanced disclosure requirements regarding cybersecurity risk management, strategy, governance and incident reporting for public companies. The SEC first released the proposed rules in March 2022 and initiated a comment period. The final rules reflect a less stringent regime than initially proposed. The amendments call for (1) real-time disclosure of cybersecurity incidents on Form 8-K or Form 6-K, as applicable, and (2) annual disclosure of an issuer's cybersecurity risk assessment processes and the respective roles of its board of directors and management in overseeing and managing cybersecurity threats. There are no scaled disclosure accommodations for smaller reporting companies ("SRCs") or emerging growth companies, though smaller reporting companies will have additional time to comply with the new real-time disclosure requirements. The rules apply to both domestic operating companies and foreign private issuers ("FPIs").

Summary of the Amendments

Incident Reporting

Pursuant to new Item 1.05 of Form 8-K, an issuer will be required to disclose certain key details regarding *material* cybersecurity incidents within four business days of the issuer's determination that it has experienced a material cybersecurity incident. The item calls for disclosure regarding the timing of the incident as well as a description of its nature and scope and the material impact or reasonably likely material impact on the company. Information regarding whether the incident has been remediated or is being remediated or regarding whether data was stolen is not required under the final rules. The final rules enable an issuer to delay filing a Form 8-K reporting a material cybersecurity incident if the United States Attorney General makes a determination that timely reporting would "pose a substantial risk for national security or public safety."

The amendments call for the issuer to make the materiality determination "without unreasonable delay" upon discovery, and utilizes the standard securities law definition of materiality (i.e., information is material

if "there is a substantial likelihood that a reasonable shareholder would consider it important" in making an investment decision, or if it would have "significantly altered the 'total mix' of information made available."). Notably, the rules specify that issuers need not include "specific or technical information" regarding their cybersecurity systems or potential weaknesses. In addition, a failure to make timely Item 1.05 disclosure will not impact an issuer's Form S-3 eligibility.

To the extent that certain information called for by Item 1.05 is not determinable at the time of filing, issuers will be required to file an amended Form 8-K. The amendment requirements do not obligate issuers to otherwise update their prior statements.

For FPIs, cybersecurity incidents will be reported on Form 6-K.

The SEC determined not to adopt requirements that issuers include disclosure in their quarterly or annual filings regarding material changes, additions or updates to the information filed via Item 1.05 of Form 8-K.

Disclosure Regarding Risk Management, Strategy and Governance

Issuers will now be required to provide Form 10-K or Form 20-F, as applicable, disclosure regarding their cybersecurity risk management and strategy as well as regarding their cybersecurity governance. The final rules are notably less cumbersome than the proposed version. Under the new regime, issuers will need to provide the disclosure required by Item 106 of Regulation S-K, which includes: (1) a description of their board of director's role in the oversight of risk stemming from cybersecurity threats, including the role of any committees or sub-committees therein, and (2) a description of the management team's role and expertise in handling *material* cybersecurity risks.

Issuers will not be required to discuss any individual director's cybersecurity expertise as had been originally proposed.

Timing

The final rules will become effective as of 30 days after their publication in the Federal Register. Issuers will be required to comply with the real-time disclosure requirements via Form 8-K or Form 6-K, as applicable, by the later of 90 days after the rules' publication in the Federal Register or December 18, 2023. SRCs can take advantage of a delayed compliance deadline of the later of 270 days from the effective date of the rules or June 15, 2024 to comply with new Item 1.05 of Form 8-K. Issuers must include Item 106 disclosure in their annual reports for fiscal years ending on or after December 15, 2023.

Next Steps

Issuers should be preparing for the amendments' effectiveness now, including by:

- Educating the board of directors on the new rules;
- Reviewing boards' and management's cybersecurity oversight and expertise, and bolstering any gaps;
- Integrating cybersecurity into the company's compliance regime;
- Developing appropriate cybersecurity expertise at all levels;
- Building and reinforcing clearly defined escalation processes;

- Developing and updating incident response and notification guidelines, including identifying what "materiality" means for the issuer; and
- Consulting with experienced legal counsel throughout the process.

We will be publishing a further discussion of the new cybersecurity rules as well as a summary of recent cyber-related SEC enforcement actions in the coming weeks.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

Sean Donahue
1.202.551.1704 / 1.212.318.6764
seandonahue@paulhastings.com

Brad Bondi
1.202.551.1701 / 1.212.318.6601
bradbondi@paulhastings.com

Ken Herzinger
1.415.856.7040
kennethherzinger@paulhastings.com

Jeremy Berkowitz
1.202.551.1230
jeremyberkowitz@paulhastings.com

Aaron Charfoos
1.312.499.6016
aaroncharfoos@paulhastings.com

Spencer Young
1.858.458.3026
spenceryoung@paulhastings.com

Stay Current is published solely for the interests of friends and clients of Paul Hastings LLP and should in no way be relied upon or construed as legal advice. The views expressed in this publication reflect those of the authors and not necessarily the views of Paul Hastings. For specific information on recent developments or particular factual situations, the opinion of legal counsel should be sought. These materials may be considered ATTORNEY ADVERTISING in some jurisdictions. Paul Hastings is a limited liability partnership. Copyright © 2023 Paul Hastings LLP.