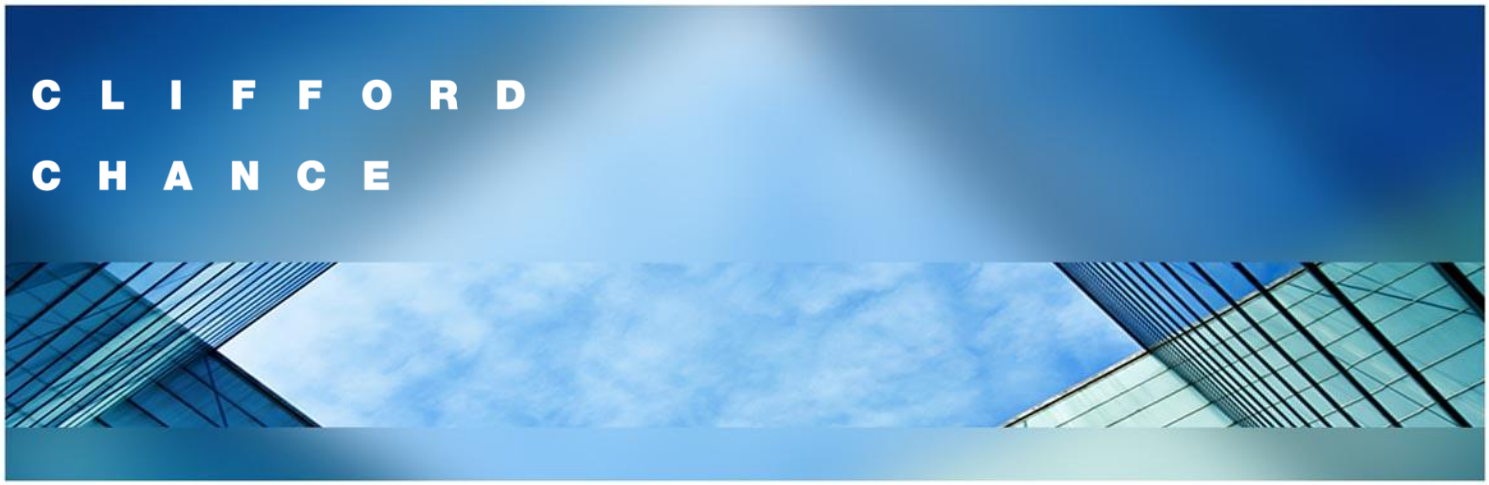

SEC ADOPTS NEW CYBERSECURITY DISCLOSURE REQUIREMENTS FOR PUBLIC COMPANIES

On July 26, 2023, the U.S. Securities and Exchange Commission (**SEC**) adopted new cybersecurity related disclosure requirements that will apply to public companies that are subject to periodic reporting obligations under US federal securities law (**registrants**). The SEC is amending Form 8-K to require registrants that use this form to report specified information related to a cybersecurity incident within four business days of determining that the incident is material. The SEC is also amending Form 6-K to require registrants that qualify as foreign private issuers (**FPIs**) to promptly furnish information related to a material cybersecurity incident when specified conditions are met. In addition, registrants will be required to include disclosures regarding cybersecurity risk management, strategy, and governance in their annual reports. Asset-backed issuers, which typically are special purpose vehicles with limited activities, are exempt from these disclosure requirements.

Key takeaways

- Registrants will be required to report specified information regarding material cybersecurity incidents using Form 8-K (or Form 6-K, if applicable) beginning on December 18, 2023.
- A registrant's materiality determination regarding a cybersecurity incident must be made without unreasonable delay after discovery of the incident.
- Registrants will be required to provide specified disclosures related to cybersecurity risk management, strategy and governance in annual reports for fiscal years that end on after December 15, 2023.
- To prepare for compliance, public companies will want to consider developing new disclosure controls and procedures to facilitate compliance and review their policies related to cybersecurity risk management.

The related rule and form amendments will become effective 30 days after publication of the SEC's release, available here, in the Federal Register (which we expect will occur in the near future), subject to the following compliance phase-in schedule:

- Registrants must begin complying with the incident disclosure requirements using Form 8-K (or Form 6-K, if applicable) beginning on **December 18, 2023**, except that registrants that qualify as "smaller reporting companies" will have the benefit of an additional 180 days.
- Registrants must begin complying with the new disclosure requirements related to cybersecurity risk management, strategy, and governance beginning with annual reports on Form 10-K (or Form 20-F, if applicable) for fiscal years ending on or after **December 15, 2023**.

- All registrants must tag these new cybersecurity disclosures using Inline XBRL beginning **one year after the applicable initial compliance date**.

BACKGROUND

In recent years, cybersecurity attacks on public companies have increased in both number and severity, posing a threat to these companies, their investors and other market participants. Although existing SEC guidance advises registrants to provide timely disclosure about material cybersecurity risks and incidents in their periodic and annual reports, the SEC has been concerned about under-reporting. In addition, voluntary cybersecurity risk management, strategy, and governance disclosures have lacked standardization and consistency, reducing their comparability and usefulness for investors. The purpose of these new cybersecurity related disclosure requirements is to ensure investors and other market participants receive timely, decision-useful information about registrants' material cybersecurity incidents, and periodic information on registrants' approaches to cybersecurity risk management, strategy, and governance that is standardized and comparable across registrants.

CYBERSECURITY INCIDENT REPORTING

Registrants will be required to report material cybersecurity incidents within four business days of determining the incident is material. In addition, they will be required to subsequently update their incident disclosures by amending their reports.

What types of incidents will need to be reported?

The SEC has defined "cybersecurity incident" to mean an unauthorized occurrence, or a series of related unauthorized 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. Registrants will need to report "material" cybersecurity incidents. An incident will 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 result from a "well-reasoned, objective approach," considering all relevant facts and circumstances, including both quantitative and qualitative factors.

What information will need to be reported?

Reporting companies will be required to describe:

- the material aspects of the nature, scope, and timing of the cybersecurity incident; and
- the material impact (or reasonably likely material impact) on the registrant, including its financial condition and results of operations.

In the guidance accompanying the final rule, the SEC explained that material impacts could include harm to a company's reputation, customer or vendor

relationships, or competitiveness, as well as the possibility of litigation or regulatory investigation or actions.

The instructions to this new reporting requirement indicate that a registrant need not disclose any specific or technical information about its planned response to the incident or its cybersecurity systems, related networks and devices, or potential system vulnerabilities in such detail as would impede the registrant's response or remediation of the incident.

When will cybersecurity incident reports need to be submitted to the SEC?

Reporting companies that use Form 8-K will be required to disclose material cybersecurity incidents to the public within four business days of making a determination that the cybersecurity incident is material. While the SEC recognizes that this type of determination may be made later than the date on which the registrant becomes aware that a cybersecurity incident has occurred, the materiality determination must be made without unreasonable delay. In addition, companies will need to amend their Form 8-K disclosures within the four business days after relevant new material information is determined or becomes available.

For context, this four-business-days reporting deadline is slightly longer than the deadlines in 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 of a cybersecurity incident within 72 hours. Federal banking regulators recently issued a final rule requiring notification within 36 hours after determining the incident has occurred,[1] and the SEC has proposed rules for registered investment advisers and funds would require notification within 48 hours of having a reasonable basis to conclude that an incident has occurred or is occurring.[2] That being said, many U.S. state incident reporting requirements provide for a longer time frame using more subjective criteria (e.g., "without unreasonable delay"). Also of note is that the SEC's rule involves disclosure to the public, whereas these other reporting requirements involve providing notification to applicable regulatory authorities.

An ongoing investigation (internal or external) will not constitute a valid reason to delay public reporting once a registrant has determined that the cybersecurity incident is material. This new reporting requirement does, however, include a time-limited delay for disclosures if the US Attorney General notifies the SEC in writing that disclosure of the incident would pose a substantial risk to national security or public safety. In addition, pursuant to existing Rule 0-6 under the Exchange Act, no publicly filed reports should include information that has been classified by an appropriate department or agency of the US federal government for the protection of the interest of national defense or foreign policy. Registrants who omit information from Form 8-K filings pursuant to Rule 0-6 will not need to separately arrange for a written notification by the US Attorney General to the SEC.

To accommodate registrants that are also required to comply with the US Federal Communication Commission's rules related to disclosing cybersecurity incidents,

1 For more on this rule, see our briefing available here.
2 For more on these proposed rules, see our briefing available here.

the SEC will allow these registrants to delay filing a Form 8-K to disclose a material cybersecurity incident for up to seven business days, subject to certain conditions.

Will there be consequences for untimely or deficient reporting?

An untimely filing of a cybersecurity incident report on Form 8-K will not, by itself, cause a company to become ineligible to file short-form registration statements using Form S-3.

The SEC has designated material cybersecurity incident reporting using Form 8-K as eligible for a limited safe harbor exemption for purposes of liability under Section 10(b) of the Exchange Act and related Rule 10b-5 (which make it illegal to make materially misleading statements, omissions, or misrepresentations in disclosures, among other things). This limited safe harbor allows reporting companies to avoid liability from penalties under Section 10(b) and Rule 10b-5 for failure to timely file a Form 8-K.

CYBERSECURITY RISK MANAGEMENT, STRATEGY, AND GOVERNANCE DISCLOSURE REQUIREMENTS FOR ANNUAL REPORTS

The SEC also adopted new annual report disclosure requirements related to cybersecurity risk management, strategy, and governance.

Form 10-K will refer to new Item 106 of Regulation S-K to require registrants to describe their processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes. This disclosure should address, as applicable, the following non-exclusive list of items:

- whether and how those processes have been integrated into the registrant's overall risk management system or processes;
- whether the registrant engages third parties in connection with any such processes;
- whether the registrant has processes to oversee and identify risks associated from cybersecurity threats associated with its use of any third-party service provider.

In addition, registrants will be required to describe in their annual reports whether any risks from cybersecurity threats (including as a result of previous cybersecurity incidents) have materially affected or are reasonably likely to affect the registrant, including its business strategy, results of operations, or financial condition and if so, how.

Registrants will also be required to describe its board's oversight of risks from cybersecurity threats and its management's role in assessing and managing these risks. This disclosure should address, as applicable, the following non-exclusive list of items:

- whether and which management positions or committees are responsible for assessing and managing such risks, and the relevant expertise of

such persons or members in such detail as necessary to fully describe the nature of the expertise;

- the processes by which such persons or committees are informed about and monitor the prevention, detection, mitigation, and remediation of cybersecurity incidents; and
- whether such persons or committees report information about such risks to the board of directors or a committee or subcommittee of the board of directors.

COMPARABLE REQUIREMENTS FOR FOREIGN PRIVATE ISSUERS

The SEC is amending Form 6-K to require a registrant that qualifies as an FPI to promptly furnish information that is material with respect to the registrant and its subsidiaries concerning material cybersecurity incidents that it:

- makes or is required to make public pursuant to the law of its home jurisdiction; or
- files or is required to file with a stock exchange on which its securities are traded and which was made public by that exchange; or
- distributes or is required to distribute to its security holders.

FPI registrants that file annual reports on Form 20-F will also be required to provide cybersecurity risk management, strategy, and governance disclosures in their annual reports on Form 20-F pursuant to a new Item 16K. The SEC did not adopt similarly comparable prescriptive cybersecurity disclosure requirements for Canadian registrants that file annual reports on Form 40-F. These companies follow Canadian disclosure standards and are already subject to the Canadian Securities Administrators' 2017 guidance on the disclosure of cybersecurity risks and incidents.

TAKEAWAYS

The SEC's newly adopted rule and form amendments impose significant new disclosure burdens on companies that are subject to the SEC's periodic reporting requirements.

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. Companies may be judged against their competitors on how they are managing cybersecurity risks.

Registrants other than "smaller reporting companies" will need to begin complying with current reporting requirements concerning material cybersecurity incidents as early as December 18, 2023. Smaller reporting companies will have an additional 180 days to prepare for compliance with the incident reporting requirements. In addition, the new cybersecurity strategy, risk management and governance disclosure requirements will apply to any annual reports (Form 10-K or 20-F) that are filed for fiscal years ending on or after December 15, 2023.

Registrants should consider taking steps now to ensure future compliance, such as:

- updating disclosure controls and procedures to provide for a process to evaluate the materiality of cybersecurity incidents and to facilitate timely reporting of material cybersecurity incidents;
- 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;
- assessing relevant cybersecurity expertise at the senior management level; and
- conducting risk assessments to identify and mitigate any cybersecurity vulnerabilities.

Clifford Chance has published a number of resources to help companies protect themselves from cyber-attacks and comply with international reporting requirements, such as our Ransomware Playbook. Also visit Clifford Chance's Talking Tech Cyber hub for cybersecurity news from around the world, as well as our Tech Trends 2023 page where we discuss cutting-edge issues relating to cybersecurity and technology.

CONTACTS

AMERICAS

Gary Brooks
Partner

T +1 212 878 8242
E gary.brooks@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

Mariana Estévez
Partner

T +1 212 878 8251
E mariana.estevez@cliffordchance.com

Jake Farquharson
Partner

T +1 212 878 3302
E jacob.farquharson@cliffordchance.com

Steven Gatti
Partner

T +1 202 912 5095
E steven.gatti@cliffordchance.com

Megan Gordon
Partner

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

Patrick Jackson
Partner

T +55 11 3019 6017
E patrick.jackson@cliffordchance.com

Devika Kornbacher
Partner

T +1 713 821 2818
E devika.kornbacher@cliffordchance.com

Trevor Lavelle
Partner

T +1 713 821 2828
E trevor.lavelle@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

Jason Parsont
Partner

T +1 212 878 8213
E jason.parsont@cliffordchance.com

Daniel Silver
Partner

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

Hugo Triaca
Partner

T +1 212 878 3222
E hugo.triaca@cliffordchance.com

Kathleen Werner
Partner

T +1 212 878 8526
E kathleen.werner@cliffordchance.com

Jonathan Zonis
Partner

T +1 212 878 3250
E jonathan.zonis@cliffordchance.com

Benjamin Berringer
Counsel

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

www.cliffordchance.com

Clifford Chance, 31 West 52nd Street, New York, NY 10019-6131, USA

Clifford Chance US LLP

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Delhi • Dubai • Düsseldorf • Frankfurt • Hong Kong • Houston • Istanbul • London • Luxembourg • Madrid • Milan • Munich • Newcastle • New York • Paris • Perth • Prague • Riyadh • Rome • São Paulo • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

AS&H Clifford Chance, a joint venture entered into by Clifford Chance LLP.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.

Tae Ho Cho
Counsel

T +1 212 878 8506
E taeho.cho
@cliffordchance.com

Matt Worden
Counsel

T +1 212 878 4970
E matt.worden
@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

APAC

Gareth Deiner
Partner

T +65 6410 2202
E gareth.deiner
@cliffordchance.com

Liu Fang
Partner

T +852 2825 8919
E fang.liu
@cliffordchance.com

Jean Thio
Partner

T +65 6506 1956
E jean.thio
@cliffordchance.com

Alan Yeung
Partner

T +852 2826 3520
E alan.yeung
@cliffordchance.com

Stephanie J. Liman
Counsel

T +65 6506 1955
E stephanie.liman
@cliffordchance.com

Erxin Lu
Counsel

T +86 10 6535 4906
E erxin.lu
@cliffordchance.com

Terrence Moloney
Counsel

T +61 2 8922 8559
E terrence.moloney
@cliffordchance.com

Yuling Geng
Foreign Legal Counsel

T +852 2825 8926
E yuling.geng
@cliffordchance.com

EUROPE

Alex Bafi
Partner

T +33 1 4405 5267
E alex.bafi
@cliffordchance.com

Jill Concannon
Partner

T +44 207006 1142
E jill.concannon
@cliffordchance.com

Michael Dakin
Partner

T +44 207006 2856
E michael.dakin
@cliffordchance.com

Dr. George Hacket
Partner

T +49 69 7199 3103
E george.hacket@cliffordchance.com

Johannes Juette
Partner

T +44 207006 5015
E johannes.juette@cliffordchance.com

Drew Rundus
Partner

T +44 207006 2875
E drew.rundus@cliffordchance.com

Olivier Plessis
Counsel

T +33 1 4405 5487
E olivier.plessis@cliffordchance.com

Dr. Axel Wittmann
Counsel

T +49 69 7199 1528
E axel.wittmann@cliffordchance.com

Laura Scaglioni
Counsel

T +39 02 8063 4254
E laura.scaglioni@cliffordchance.com