SANGRA MOLLER LLP
Barristers & Solicitors

LEGAL CURRENCY
A Client Communication

U.S. Securities and Exchange Commission Adopts New Cybersecurity Disclosure Rules for U.S. Public Companies and Foreign Private Issuers

On July 26, 2023, the U.S. Securities and Exchange Commission ("**SEC**") adopted final rules and amendments mandating disclosure related to cybersecurity risk management, strategy, governance, and incident reporting (the "**Rules**"). These new Rules generally apply to most domestic SEC reporting issuers, and foreign private issuers ("**FPIs**") that report using Form 20-F.

Under the new framework, U.S. domestic issuers and FPIs must:

- report certain details of a material cybersecurity incident (the "**Incident Disclosure Requirement**"); and
- describe their cybersecurity risk management, strategy and governance practices in their annual reports (the "**Risk Management Disclosure Requirements**").

The Risk Management Disclosure Requirements do not extend to Canadian issuers who report using Form 40-F under the U.S.-Canada Multijurisdictional Disclosure System. However, Form 40-F filers must provide information on Form 6-K regarding any material cybersecurity incidents they disclose or make public in a foreign jurisdiction, to any stock exchange, or to their security holders.

Effective Dates

All corporate registrants, except for small reporting companies, are required to comply with the Incident Disclosure Requirement beginning on **December 18, 2023**. Smaller reporting companies have an additional 180-day grace period and must commence compliance with the Incident Disclosure Requirement starting on **June 15, 2024**.

The Risk Management Disclosure Requirements will be mandatory in annual reports for fiscal years ending on or after **December 15, 2023**. Therefore, companies with calendar-year ends must adhere to the new Risk Management Disclosure Requirements in their 2023 reports.

Cybersecurity Incident Reporting Requirement Rule

The new Incident Reporting Requirement mandates that U.S. domestic issuers report material cybersecurity incidents on Form 8-K. FPIs must provide information on material cybersecurity incidents that they disclose or otherwise publicize in a foreign jurisdiction, to any stock exchange or to security holders using Form 6-K.

A "cybersecurity incident" is defined as 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." "Accidental" occurrences are to be considered "unauthorized," even in the absence of confirmed malicious activity.

U.S. domestic issuers' disclosure under the new Incident Reporting Requirement should encompass the material aspects of the incident, including its:

- nature, scope, and timing; and
- impact or reasonably likely impact.

Materiality is to be assessed in line with the general principles of determining materiality for securities law purposes. Generally, information is considered material if there is a substantial likelihood that a reasonable shareholder would find it important when making an investment decision, or if its disclosure would significantly alter the total mix of information available to investors. This could, for example, include qualitative material impact, such as reputational harm, in addition to a strictly financial or quantitative materiality analysis.

SEC Form 8-K has been amended to add Item 1.05, which requires disclosure of a material cybersecurity incident within four business days of determining that the incident

is material. However, in cases such as where the United States Attorney General deems that immediate disclosure would pose a substantial risk to national security or public safety, filing may be delayed.

Crucially, the company's determination of a cybersecurity incident's materiality is what triggers the Form 8-K Incident Reporting Requirement, not the date of discovery of the incident. This approach aims to focus disclosure on incidents that are truly material to investors. The Incident Disclosure Rule will require issuers to describe the material aspects of the cybersecurity incident, including its nature, scope, timing, and material impact (or reasonably likely material impact) on the issuer. This impact assessment should consider various factors, not limited to financial aspects, but also qualitative factors like customer and vendor relationships, reputation, competitiveness, and potential litigation.

The Form 8-K Incident Reporting Requirement states that companies must make the materiality determination "without unreasonable delay," and they should not delay making a materiality determination simply because they can't yet ascertain the full extent of the incident. As a practical step, companies that discover an incident should promptly engage external legal counsel, forensic cyber experts, and other relevant professionals to investigate and gather the necessary facts for the materiality determination.

Even if some required information isn't available at the time of the initial Form 8-K filing, issuers must still meet the four-business-day deadline. In cases where missing information later becomes available, an amended Form 8-K must be filed.

For FPIs, Form 6-K has been amended to include "material cybersecurity incidents" as a triggering item for filing requirements when such information is disclosed in a foreign jurisdiction, to any stock exchange, or to its security holders. Consistent with other disclosure requirements set out in Form 6-K, the amendments to Form 6-K do not specify the details to be disclosed about such incidents. Instead, the form and content of cybersecurity incident disclosure attached to Form 6-K will generally be determined by the disclosure requirements of the FPI's home country.

To address concerns about aiding cybersecurity threat actors, the SEC instructs issuers not to disclose overly specific or technical information about their planned response to the incident or intricate details about their cybersecurity systems.

Annual Disclosure of Cybersecurity Risk Management, Strategy and Governance

The new rules on cybersecurity-related disclosure obligations require U.S. domestic reporting companies to include disclosure in their annual reports on Form 10-K and FPIs to disclose on Form 20-F regarding both cybersecurity risk management and strategy, and cybersecurity governance.

Regarding the disclosure of risk management and strategy, the issuer is obligated to provide details about:

- the processes, if any, employed by the issuer for assessing, identifying, and managing material risks arising from cybersecurity threats; and
- whether any risks stemming from cybersecurity threats have significantly impacted or are reasonably expected to significantly impact their business strategy, financial condition, or results of operations.

To describe an issuer's procedures for assessing, identifying, and managing material cybersecurity threat risks, issuers will need to explain whether and how they have integrated their cybersecurity processes into the company’s broader risk management systems or procedures.

In order to provide investors with insight into the extent of cybersecurity functions outsourced by the issuer, the issuer must also divulge whether assessors, consultants, auditors, or other third parties are involved in their cybersecurity processes. Furthermore, issuers are required to disclose whether the company has implemented procedures to oversee and identify material risks associated with cybersecurity threats stemming from their engagement with third-party service providers.

In the context of cybersecurity governance, issuers are required to provide the following descriptions:

- the board’s oversight of cybersecurity threats, including the identification of any board committee or subcommittee responsible for managing risks related to cybersecurity threats, and the process by

which the board or relevant committee receives information about these risks; and

- the role and expertise of the management team in assessing and managing material cybersecurity risks, as well as in implementing the company's cybersecurity policies, procedures, and strategies. This should include:
    - identification of specific management positions or committees responsible for assessing and managing such risks, along with a description of the relevant expertise of these individuals or committee members, provided in enough detail to fully convey the nature of their expertise;
    - an outline of the processes by which these individuals or committees stay informed about and monitor activities related to the prevention, detection, mitigation, and remediation of cybersecurity incidents; and
    - disclosure of whether these individuals or committees are responsible for reporting information about cybersecurity risks to the board of directors or a specific committee or subcommittee within the board of directors.