ASSOCIATION DES BANQUIERS CANADIENS
CANADIAN BANKERS ASSOCIATION

Darren Hannah
Vice-President
Finance, Risk & Prudential Policy

Tel (647) 730-4760
dhannah@cba.ca

May 5, 2022

Via Email

Ms. Vanessa Countryman,
Secretary,
U.S. Securities and Exchange Commission,
100 F Street,
Washington, DC 20549-1090,
United States.

Re: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure (File No. S7-09-22)

Dear Ms. Countryman:

The Canadian Bankers Association (the "CBA") welcomes the opportunity to comment on the recently proposed rules of the U.S. Securities and Exchange Commission (the "SEC") on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure (Release Nos. 33-11038; 34-94382; IC-34529; File No. S7-09-22) (the "Proposed Rules").

The CBA is a professional industry association that provides information, advocacy education and operational support services to its membership of more than 60 domestic and foreign banks operating in Canada. The CBA provides governments and others with a centralized contact for matters relating to banking in Canada, and advocates for public policies that contribute to a sound, thriving banking system to ensure Canadians can succeed in their financial goals. A number of the CBA's members are also foreign private issuers ("FPIs") listed on national securities exchanges in the United States and subject to U.S. periodic reporting requirements under the Securities Exchange Act of 1934, as amended (the "Exchange Act"). The SEC's multijurisdictional disclosure system ("MJDS") for Canadian issuers allows eligible Canadian issuers to register securities under the U.S. Securities Act of 1933, as amended (the "Securities Act") and to register securities and satisfy their reporting obligations under the Exchange Act by use of documents prepared largely in accordance with Canadian requirements.

We note that in the release proposing the Proposed Rules (the "Proposing Release"), the SEC specifically addresses Canadian MJDS registrants and requests comments on whether the SEC should amend Form 40-F to require such registrants to comply with the Proposed Rules in the same manner as Form 10-K (for U.S. domestic registrants) or Form 20-F (for non-MJDS FPIs) filers. In response to this request for comment, we believe, consistent with the SEC's existing and longstanding approach to disclosure requirements applicable to MJDS registrants, that such registrants should be excluded from any incremental cybersecurity disclosure requirements in connection with their annual reports on Form 40-F.

We note that the Proposed Rules would require all in-scope issuers (including non-MJDS FPIs) to disclose: (i) their policies and procedures to identify and manage cybersecurity risks (including whether they consider cybersecurity risks as part of their business strategy, financial planning and capital allocation); (ii) the board of directors' and management's role in cyber governance; and (iii) cyber expertise of any member of the board of directors in their periodic reports on Forms 10-K and 10-Q (for U.S. domestic issuers) and Form 20-F (for non-MJDS FPIs).

We believe that applicable Canadian annual and interim disclosure requirements are sufficient to ensure investors receive material information regarding material cybersecurity incidents, and cybersecurity risk management, strategy and governance. See the discussion under "Background on the Canadian Regulatory Framework" below. As a result, there is no reason for the SEC to depart from the longstanding MJDS principle of deference to Canadian disclosure requirements, and MJDS registrants should be exempt from the Proposed Rules in all circumstances.

Background on the Canadian Regulatory Framework

We note that the policy considerations underlying the Proposed Rules are frequently addressed under home country corporate, stock exchange or other requirements. This is certainly the case with respect to MJDS registrants. For example, the Canadian Securities Administrators (the "CSA") identified cybersecurity as a priority area in the CSA's 2016-19 Business Plan and have maintained their focus in this area.

The CSA has accordingly published a series of notices outlining disclosures that should be made in respect of material cybersecurity incidents, and risks and related mitigation strategies (collectively, the "Staff Notices").[1] The Staff Notices set out, among other things, the CSA's expectations that each registrant will: (i) adopt cybersecurity policies and procedures which govern the use of electronic communications and devices, network security and the verification of client instructions sent electronically; (ii) require frequent training of all employees, including with respect to risk recognition, types of cyber threats and incident escalation; (iii) conduct an annual risk assessment process; (iv) prepare an incident response plan; (v) oversee the cybersecurity practices of service providers that have access to firm networks or data; (vi) implement data protection safeguards, including the use of encryption and passwords on all computers and electronic devices; and (vii) maintain insurance that adequately covers cybersecurity risks.

Furthermore, as part of ongoing efforts by the CSA to highlight cybersecurity risks for issuers, registrants and other regulated entities, the British Columbia Securities Commission, the Ontario Securities Commission and the *Autorité des Marchés Financiers* (Quebec) published a multilateral staff notice with respect to disclosure of cyber security risks and incidents (the "Multilateral Staff Notice").[2] The Multilateral Staff Notice recognizes that any disruptions due to cybersecurity incidents could adversely affect the

---

1 CSA Staff Notice 11-326, *Cyber Security* (September 26, 2013); CSA Staff Notice 11-332, *Cyber Security* (September 27, 2016); CSA Staff Notice 33-321, *Cyber Security and Social Media* (October 19, 2017).

2 Multilateral Staff Notice 51-347, *Disclosure of Cyber Security Risks and Incidents* (January 19, 2017).

business, results of operation and financial condition of issuers, and provides guidance on risk factor disclosure to a variety of issuers across different industries.

Similar to the Proposed Rules, the Staff Notices and Multilateral Staff Notice focus on governance and incident disclosure in connection with cybersecurity.

- *Cyber Incident Disclosure*: A cybersecurity incident must be disclosed in accordance with securities legislation if it is a material fact or material change to the issuer's business.[3] When determining the materiality of a cybersecurity incident, the CSA notes that there is no bright-line test and the threshold at which a cybersecurity incident becomes material will vary between issuers and industries. The materiality determination (which is necessarily a dynamic process that runs through the detection, assessment and remediation phases) requires a contextual analysis of the cybersecurity incident. For instance, an isolated cybersecurity incident may not be material but a series of minor incidents may become material, depending on the type and magnitude of disruption caused.

- *Cyber Governance (and Risk Mitigation)*: On an ongoing basis, the CSA discusses cybersecurity policies and procedures with registered firms as part of compliance reviews. Areas of focus include: (i) cyber security risk assessment and information security governance programs; (ii) IT safeguards and controls; (iii) use of encryption; (iv) risks related to third-party service providers; (v) vulnerability tests and compliance monitoring; (vi) evidence of regular employee training and awareness; (vii) incident response plans; and (viii) practices for accepting client instructions to withdraw or transfer funds via electronic means.[4]

The CSA states that its cybersecurity Staff Notices apply to all registered issuers regardless of their size, how recently they were registered or the extent to which they rely on service providers or affiliates for their cybersecurity safeguards.

Furthermore, the members of the CBA, in their capacity as financial institutions (particularly, members that are Federally Regulated Financial Institutions ("FRFIs") – all CBA members that file periodic disclosure reports with the SEC are FRFIs), are subject to an additional layer of regulatory requirements and guidelines in relation to cybersecurity (incident) disclosure and governance imposed by financial and industry regulators in Canada, including the Investment Industry Regulatory Organization of Canada (IIROC)[5],

---

3 The issuer should refer to the guidance in National Policy 51-201 *Disclosure Standards* and may in addition refer to the provisions of Part 1(f) of Form 51-102F1 *Management's Discussion & Analysis* and Part 1(e) of Form 51-102F2 *Annual Information Form* of National Instrument 51-102 *Continuous Disclosure Obligations* (see Multilateral Staff Notice, page 607 (40 OSCB)).

4 CSA Staff Notice 11-332, *Cyber Security* (September 27, 2016).

5 Section 3703 (*Reporting by a Dealer Member to IIROC*), IIROC Incident Reporting (available at https://www.iiroc.ca/rules-and-enforcement/iiroc-rules/3000/3703-reporting-dealer-member-iiroc); IIROC *Fundamentals of Technology Risk Management* dated March 31, 2021; IIROC Notice on *Cybersecurity – Ransomware* dated March 16, 2021; IIROC Notice on *Cybersecurity and Fraud – Protecting Clients* dated November 9, 2020; IIROC Notice on *Cloud Services and*

the Mutual Fund Dealers Association (MFDA)[6] and the Office of the Superintendent of Financial Institutions (OSFI). OSFI is the primary prudential regulator for FRFIs, and recently issued a release with respect to Technology and Cyber Security Incident Reporting detailing reporting criteria, initial notification requirements and subsequent reporting requirements.[7] This release provides, among other things, that FRFIs must report a technology or cyber security incident to OSFI's Technology Risk Division as well as their lead Supervisor at OSFI within 24 hours (or sooner if possible). OFSI is also in the process of finalizing its Draft Guideline B-13 on Technology and Cyber Risk Management, which sets out OSFI's expectations for sound technology and cyber risk management across five domains (i.e., Governance and Risk Management, Technology Operations, Cyber Security, Third-Party Provider Technology and Cyber Risk, and Technology Resilience).[8]

The foregoing demonstrates that the Canadian securities and financial industry regulators view cybersecurity as an important priority, and as a result, have released or are in the process of releasing multiple cybersecurity (incident) disclosure and governance requirements and guidelines.

Exemption for MJDS Registrants

We note that while the SEC is not proposing any changes to Form 40-F, which governs the annual reports filed by MJDS registrants with the SEC, it is seeking comment on whether it should require MJDS registrants to comply with cybersecurity-related disclosure requirements in the same manner as Form 10-K and 20-F filers (potentially, through an amendment to Form 40-F). Cybersecurity periodic reporting requirements are proposed to be added as a new Item 106 of Regulation S-K and Item 16J of Form 20-F, and through an amendment to Item 407 of Regulation S-K. We request that, in the event the SEC adopts the new Item 106 of Regulation S-K and Item 16J of Form 20-F and amends Item 407 of Regulation S-K, the SEC expressly acknowledge that MJDS registrants will be exempt from the new disclosure requirements, consistent with the statement in the Proposing Release to such effect.

Application Interfaces dated June 24, 2020; IIROC Notice on *COVID-19 and Cybersecurity – Tips for Advisors and Employees* dated April 21, 2020; IIROC Notice on *COVID-19 and Cybersecurity* dated March 30, 2020; IIROC *Cyber Governance Guide* dated March 3, 2020 (IIROC notices are available at https://www.iiroc.ca/members/cybersecurity-technology).

6 MFDA Policy No.6 on *Information Reporting Requirements* dated March 17, 2016 (available at https://mfda.ca/policy/policy06/); MFDA Bulletin on *Cybercriminals Currently Exploiting the COVID-19 Pandemic* dated March 19, 2020, #0816-M (available at https://mfda.ca/bulletin/bulletin0816-m/); MFDA Bulletin on *Cybersecurity* dated May 19, 2016, #0690-C (available at https://mfda.ca/bulletin/bulletin0690-c/).

7 OFSI *Technology and Cyber Security Incident Reporting*, effective as of August 13, 2021 (available at https://www.osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/adv-prv/Pages/TCSIR.aspx).

8 The proposed Guideline B-13 is designed to complement existing Guidelines E-21 (*Operational Risk Management*) and B-10 (*Outsourcing of Business Activities, Functions and Processes*), as well as its Technology and Cyber Incident Reporting Policy and its Cyber Security Self-Assessment tool (see OFSI Draft Guideline B-13 on *Technology and Cyber Risk Management* (available at https://www.osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/gl-ld/Pages/b13.aspx)).

We believe imposing additional cybersecurity disclosure requirements on MJDS registrants would result in significant inefficiencies, inconsistencies and incremental costs as well as unnecessary duplication of administrative effort by MJDS FPIs subject to multiple different cybersecurity disclosure regimes. As described above, Canadian issuers are already subject to home country requirements and guidelines with respect to cybersecurity disclosure. Deference to home country practice in respect of such disclosure and governance matters has historically been viewed by MJDS FPIs as minimizing the risk of such inconsistent and/or overlapping requirements and guidelines. Extension of the Proposed Rules to issuers already subject to substantially similar requirements would be viewed as a step in the wrong direction for the efficiency of global capital markets and be contrary to the principles of MJDS.

Other Concerns with the Scope of the Proposed Rules

In the event that the final rule requires MJDS registrants to comply with cybersecurity-related disclosure requirements in the same manner as Form 10-K and 20-F filers, which the CBA strongly opposes, we have four significant concerns with the Proposed Rules as drafted.

First, we believe that not all of the proposed required disclosures are necessarily material (or even helpful) to inform investors, as some disclosures are likely to be vague, overbroad or even potentially misleading at the time required to be made under the Proposed Rules due to the difficulty of capturing the complexities of a cyber threat or attack in a very short period of time, and as a result may accomplish more harm than good (including potentially exposing registrants to unwarranted litigation risks). This is particularly true when registrants are required to disclose ongoing and unremediated cybersecurity incidents which may involve even greater risks and harms to such registrants, their customers and businesses and, by extension, their shareholders and other market participants. The SEC argues in the Proposing Release that these risks and harms are outweighed by the benefit of publicly disclosing a cybersecurity incident while it is still ongoing and unremediated.[9] However, required disclosures of ongoing and unremediated incidents poses far greater security risks in the current more advanced cyber threat environment than we believe has been anticipated by the SEC. In the experience of our members, the perpetrators of cyberattacks frequently seek to hide their presence in the network, making it difficult or impossible to identify such bad actors at the time a cybersecurity incident becomes known, and so providing such bad actors with notice will grant them an opportunity to further hide their identity and activities. In addition, immediate disclosure of ongoing and unremediated incidents will enable other bad actors to further target a registrant at a time when it is already focused on addressing a known threat. This is particularly concerning for complex financial institutions with operations in many international jurisdictions. If banks are compelled to publicly disclose ongoing or unremediated material cybersecurity incidents, or otherwise publicly disclose information about registrant's cybersecurity environment or potential system vulnerabilities so as to alert perpetrators of attacks or empower additional threat actors to gain unauthorized access to compromised systems, this could have devastating impacts on broader economic stability. In addition, we are concerned that collecting relevant information from

[9] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 87 Fed. Reg. 16590 (Mar. 23, 2022) (to be codified at 17 C.F.R. pt. 229, 232, 239, 240, and 249), at 16596.

third party service providers regarding ongoing and unremediated incidents relating to those providers will be difficult or impossible and increase the likelihood that an initial mandated disclosure is not complete or accurate. As such, we do not believe the security risks posed by disclosure of ongoing and unremediated cybersecurity incidents are outweighed by the benefit of immediate public disclosure.

Second, as complex financial institutions that routinely use third party IT service providers for their IT infrastructure, our members also have concerns that the Proposed Rules may potentially require such service providers to publicly disclose an ongoing and unremediated cyberattack. Such premature disclosure would inhibit the service provider's ability to respond and could enable bad actors to use the service provider as a vector to attack its customers before the service provider or its customers have had a chance to take remedial measures to mitigate harm. We believe that public disclosure by a critical vendor of an ongoing and unremediated incident increases the likelihood that the vendor can be leveraged by malicious cyber actors as a vector to infiltrate customers, including financial institutions and other critical infrastructure providers.

Third, the proposed Item 407(j) of Regulation S-K would require registrants to disclose whether any member of the board of directors has "cybersecurity expertise" (and, if so, the director's name and details sufficient to fully describe the nature of the expertise). We believe "expertizing" certain members of a company's board of directors also raises concerns. We believe that this disclosure requirement would exert pressure on registrants to appoint directors with such expertise, which may come at a significant cost to the ability of their boards to oversee other risks to the company without proportionate benefits, particularly at boards of heavily regulated financial institutions. Further, by appointing directors with single subject-matter expertise, registrants may experience less effective board oversight, as those with "expertise" may naturally assume responsibility over cybersecurity risk and management, which the board as a whole should oversee. The proposed responsibility allocated to the board could blur the lines between the typical or existing responsibility allocation between the board and management. Further, we wanted to note that the Proposed Rules do not include a safe harbor, which is the case in other areas that require specific expertise.

Fourth, the Proposed Rules would not permit a reporting delay for ongoing investigations, even where federal law enforcement has requested a delay and state law permits it. While the SEC's request for comment asks whether there should be a safe harbor allowing registrants to delay reporting of a cybersecurity incident where the Attorney General requests a delay from the SEC,[10] the scope of the contemplated exemption is indefensibly narrow, particularly for registrants with operations outside of the United States. In our view, there should be an exemption to permit delayed disclosure upon the request of any competent national, state or local law enforcement authority. Requiring disclosure notwithstanding the request of a reporting delay by law enforcement would

---

[10] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 87 Fed. Reg. 16590 (Mar. 23, 2022) (to be codified at 17 C.F.R. pt. 229, 232, 239, 240, and 249), at 16598. "Should any rule provide that the Commission shall allow registrants to delay reporting of a cybersecurity incident where the Attorney General requests such a delay from the Commission based on the Attorney General's written determination that the delay is in the interest of national security?"

otherwise likely result in: (i) great difficulty or impossibility for law enforcement to collect significant evidence or apprehend the bad actors; and (ii) the destruction of evidence or information that could identify the bad actors or further actual or intended victims or could assist in assessing the scope and impact of the incident (including the remedial measures).

* * *

Conclusion

Thank you for the opportunity to provide our view on the Proposed Rules. For the reasons discussed above, we respectfully believe that MJDS registrants should be exempt from any incremental cybersecurity requirements under the Proposed Rules.

Sincerely,

Darren Hannah
Vice-President, Finance Risk & Prudential Policies