IIACACCVM
INVESTMENT INDUSTRY ASSOCIATION OF CANADA
ASSOCIATION CANADIENNE DU COMMERCE DES VALEURS MOBILIÈRES

701 West Georgia Street | Suite 1500
Vancouver, BC | V7Y 1C6
604.637.1677 | www.iiac.ca

www.iiac.ca

Susan Copland, LLB, BComm
Managing Director
scopland@iiac.ca

May 22, 2018

Ms. Erica Young
Policy Counsel
Investment Industry Regulatory Organization of Canada
Suite 2000
121 King Street West Toronto, Ontario M5H 3T9
eyoung@iiroc.ca

Market Regulation
Ontario Securities Commission
Suite 1903, Box 55
20 Queen Street West
Toronto, Ontario M5H 3S8
marketregulation@osc.gov.on.ca

Dear Ms. Young:

Re: Proposed Amendments Respecting Mandatory Reporting of Cybersecurity Incidents (the "Proposed Process")

The Investment Industry Association of Canada (the "IIAC" or "Association") appreciates the opportunity to comment on the Proposed Process. While we appreciate that it is important that IIROC understand the threats facing the industry, it is not clear that the additional reporting, as it is structured, will provide benefits that exceed the costs to the industry. We believe the current reporting structure required through the Privacy Commission under the Personal Information Protection and Electronic Documents Act (PIPEDA), as well as required reporting through other regulatory bodies such as the Office of the Superintendent of Financial Institutions (OSFI) could be leveraged to provide IIROC with information, rather than creating a new, parallel system of reporting that introduces new and uncertain requirements.

In particular, we have the following concerns.

Definition of cybersecurity incident

The definition of cybersecurity incident in the Proposed Process incorporates the reporting standards that are similar to that contained in other applicable regulation, but it also adds several elements that are not clearly defined. This potentially materially expands the scope of the reporting requirement, without demonstrable benefits that would justify the additional reporting burden.

For example, the PIPEDA regulation contains a reporting requirement where there is "real risk of significant harm to the individual". Under the Act, "significant harm" is defined to include bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property. The definition in the Proposed Process includes a reporting trigger where there is a "reasonable likelihood" of an incident resulting in: "substantial harm or inconvenience to any person." This appears to expand the definition beyond what is reportable under PIPEDA, but it is not clear how "real risk" differs from "reasonable likelihood" and how "significant harm" differs from "substantial harm" and what is meant by "inconvenience", which, unless clearly defined, could broaden the requirement to make compliance impractical.

Under the OSFI *Major Cyber Security Incident Reporting* guidelines, which several of Dealer Members are subject to, Dealers are required to report incidents with the highest and second-highest severity, by the triage standard for Federally Regulated Financial Institutions. It should be noted that these members all have their own incident classification and escalation process.

In determining whether to report, OSFI requires Dealers to consider the following:

- Impact to key/critical Information Systems/Data.
- Severe operational impact to internal users.
- Significant and serious levels of system / service disruptions.
- Severe and extended disruptions to critical business systems / operations.
- Number of external customers impacted is large or growing.
- Negative reputational impact is imminent.
- Incident reported to public authorities.

The Proposed Process is unclear in explaining the rationale for expanding the scope of the reporting requirement beyond PIPEDA and OSFI federal requirements, and articulating what types of incidents are intended to be captured by this different wording. Given that this provision seems to be addressing the same type of harm (to individuals), and that the Proposed Process requires reporting where other "applicable laws" require notice to any "government body, securities regulatory authority or other self-regulatory organization, it would be useful to harmonize, or defer to PIPEDA or OSFI standards as applicable, to ensure consistency and reduce the unnecessary burden of ascertaining which organization's standards are triggered, and preparing different reports with different timing requirements for any given cybersecurity incident.

The additional IIROC requirements relating to reporting where there is a "material impact on any part of the normal operations of the Dealer member, also creates uncertainty and inconsistency with the reporting requirements under PIPEDA, and appears more stringent than OSFI requirements. Where an incident creates a material impact on the normal operations of a Dealer Member, but does not put any client data at risk or affect operations that would materially affect service to clients, it is unclear why this would require reporting. For instance, would an incident that slows down the firm's website, or internal systems be the type of matter that would be subject to the Proposed Process? We are concerned that required reporting of incidents that do not pose a risk to the firm or the client would create additional burdens for firms without commensurate benefits to the industry. We suggest that the reference to "normal operations" be qualified to ensure these operations are material to client data security.

The differences in the timing of the reports under the Proposed Process also potentially creates concerns, in that it is also different from the timing under PIPEDA and OSFI. PIPEDA requires only one report, filed "*as soon as feasible after the organization determines that the breach has occurred",* with the ability to file updates as information becomes available, and OSFI requires timely notification of major cyber security incidents. The three day IIROC requirement from discovery of the incident, may in some cases, be premature, particularly where the breach occurs over a weekend (as business days are not specified) or has significant impacts that are not known at the three day mark. In addition, the language should also reflect PIPEDA's trigger from the determination that a breach has occurred rather than the discovery of a breach. Again, parallel reporting processes with PIPEDA or OSFI so that reports filed pursuant to those requirements could be filed with IIROC on the same time line, would be helpful to ensure that firms are using their resources to deal with the cybersecurity incident in an efficient manner rather than developing different reports for different regulators with different timelines.

The 30 day follow-on report also represents an additional burden not required by other regulatory bodies. We suggest that the reporting process mirror the requirements of existing regulation, and that IIROC accept the content of those reports as specified by those regulatory bodies.

If IIROC believes it is necessary to receive specific reports with different triggers, criteria and timing from those under PIPEDA or OSFI, it is critical that the circumstances under which a report should be filed be clearly articulated, so that firms are not over or under-reporting cybersecurity incidents. The definitions of "substantial harm", "inconvenience", and "material impact" should be illustrated with examples. It should be noted that the categorization of an impact as "material" will likely vary as between very large and small firms, and this should be taken into account. It would be useful to engage in a discussion with members where firms could describe incidents, and IIROC could determine whether they should be reported. The outcome of this exercise should be articulated in guidance document accompanying the regulatory changes. Consistent with OSFI requirements, firms should also have discretion in determining what is material for their particular operation.

The Proposed Process should also be clear how cybersecurity incidents originating from a source outside the firm (such as an identity theft with the source at an unrelated retailer) that may impact a client's account are to be dealt with under this reporting process. It is our position that this is not a cybersecurity breach at the firm and as such, not subject to reporting requirements. IIROC should also specify if a firm with different divisions (eg: a Wealth Management and Securities Division) is required to submit separate reports for the same incident involving the same clients.

The IIROC Notice states that one of the objectives of the Proposed Process is to facilitate information sharing. We are concerned that such information sharing, without expertise and established protocol may expose the industry to further harm, either by notifying cybercriminals of areas of exposure, or in respect of legal liability. It may also create unnecessary alarm for clients, as notification may occur prior to understanding if, and to what extent personal data has been compromised. Given the existence of information sharing organizations with the expertise to quickly detect, analyze and anonymize information, it is unclear whether IIROC's participation in this activity would be useful, and in fact, may be detrimental.

In respect of the report filing process, it is important that the process be secure, so that information about the cybersecurity incident, including the data involved remains confidential and does not expose the reporting firm to further cyber incidents from vigilant criminals. A secure email or portal system should be developed to receive reports, in whatever format they may be sent.

We support IIROC's efforts to assist members in their cybersecurity efforts, and their objective to be informed about current industry cyber threats. It is important that these efforts do not impose additional unnecessary burdens on Dealers at a time when resources are committed to responding to cybersecurity incidents, and reporting to other regulators. In order for IIROC to receive the information it seeks on a timely basis, in a reasonably consistent manner, we suggest that it accept reports filed to under PIPEDA or OSFI requirements on the same timelines. This would ensure that IIROC receive the key information needed to understand the incidents, and Dealers not be additionally burdened drafting reports triggered by different events with slightly different formats and time requirements.

Thank you for considering our comments. If you have any questions, please don't hesitate to contact me.

Yours sincerely,

Susan Copland