IIROC OCRCVM
Investment Industry Regulatory Organization of Canada
Organisme canadien de réglementation du commerce des valeurs mobilières

IIROC NOTICE

Rules Notice
Notice of Approval/Implementation
Dealer Member Rules [IIROC Rules]

Please distribute internally to:
Institutional
Internal Audit
Legal and Compliance
Operations
Senior Management
Retail

Contact:

Erica Young
Policy Counsel
Telephone: 416.646.7211
e-mail: eyoung@iiroc.ca

19-0194
November 14, 2019

Amendments Respecting Mandatory Reporting of Cybersecurity Incidents

Executive Summary

The Canadian Securities Administrators (**CSA**) have approved amendments to the Dealer Member Rules (**DMRs**) and corresponding amendments for the IIROC Dealer Member Plain Language Rule Book (the **IIROC Rules**) to require mandatory reporting of a cybersecurity incident by Dealer Members (**Dealers**) to IIROC (the **Amendments**).

The Amendments:

- require Dealers to report to IIROC any cybersecurity incidents within three days of discovery of the cybersecurity incident,
- require Dealers to provide IIROC with an incident investigation report within 30 days of discovery of the cybersecurity incident, and
- list the information Dealers must report.

The Amendments are effective immediately.

1. Background

On April 5, 2018, we issued Notice 18-0070 requesting comments on the Amendments to the DMRs and corresponding IIROC Rules relating to mandatory reporting of cybersecurity incidents by Dealers to IIROC.

The Amendments:

- require Dealers to report to IIROC any cybersecurity incidents within three days of discovery of the cybersecurity incident,
- require Dealers to provide IIROC with an incident investigation report within 30 days of discovery of the cybersecurity incident, and
- list the information Dealers must report.

In formulating the Amendments, we sought to create a framework that would allow IIROC to:

- provide immediate support to a Dealer responding to a cybersecurity incident,
- alert other Dealers of threats and share best practices for incident preparedness,
- evaluate trends and develop comprehensive insight regarding cybersecurity, and
- promote confidence in the Dealer and the integrity of the market.

The Amendments continue IIROC's ongoing work in supporting our Dealers' cybersecurity preparedness. This work has included recent tabletop exercises and a second round of cybersecurity self-assessment surveys. We also recognize the voluntary reporting made by some Dealers since publication of Notice 18-0063 on March 22, 2018.

Since IIROC first published its Cybersecurity Incident Best Practices Guide in December 2015, cyber risks have continued to evolve and present a more urgent threat of harm to investors, market participants and Dealers. Furthermore, as IIROC seeks more ways to support industry transformation, we recognize Dealers are increasing their collection of data and reliance on complex information systems. This development highlights the importance of timely information sharing to mitigate cyber risk.

2. Comments Received

In response to the publication for comment, we received eight public comment letters. We set out below a summary of the themes of the comments received and our responses. A full summary of the comment letters received and our responses is set out in **Appendix 1** – Response to Public Comments.

2.1 Summary of Comments Received

We received public comments respecting the following themes:

- how reporting obligations in this area overlap or can be distinguished from existing reporting obligations under the *Privacy Information Protection and Electronic Documents Act* (**PIPEDA**), or its provincial equivalent, and reporting obligations to regulatory bodies such as the Office of the Superintendent of Financial Institutions (**OSFI**),
- IIROC's use of the cybersecurity incident information collected and how such information will be kept confidential, managed internally and disseminated with Dealers and the public,
- the definition of "cybersecurity incident", including clarification of the types of cybersecurity incidents that would give rise to a reporting obligation, and
- the timing of the cybersecurity incident reports and the level of information to be contained in the reports.

2.2 Summary of Response to Comments

We determined that in order to respond to the comments we received, we did not need to make material changes to the Amendments. Rather, we provide further clarification relating to the purpose and intent of the Amendments in our Response to Public Comments (see **Appendix 1**) and Frequently Asked Questions (described more fully in section 5 below).

More specifically, in our Response to Public Comments, we:

- emphasized the impact and the growing threat that cybersecurity incidents may have on investors and capital markets and the appropriateness of IIROC collecting information about these incidents,
- clarified our intent to create a broad and flexible definition of "cybersecurity incident" that accommodates the range of Dealer business models and operations,
- confirmed that any cybersecurity incident information IIROC collects will be shared with other Dealers on an anonymous and high level basis,
- clarified the distinction between the three-day and 30-day reports and acknowledged the limited information that a Dealer may possess shortly after discovery of a cybersecurity incident, and
- clarified the interpretation of the term "information system".

3. Non-Material Changes

While we did not make any material changes to the Amendments, we did make the following non-material changes:

- correction of the subsection numbering in the amendments to DMR 3100, and
- elimination of the word "inconvenience" from the definition of cybersecurity incident (and the corresponding reporting obligation) to clarify the scope of the definition of cybersecurity incident.

4. Implementation

The Amendments will be effective immediately.

5. Frequently Asked Questions

We are concurrently publishing a Frequently Asked Questions Guidance Note to assist Dealers in understanding their obligations under the Amendments (see Notice 19-0195). We intend to update periodically this document as necessary.

6. Appendices

Appendix 1 – Response to Public Comments

Appendix 2 – Text of Final Amendments to DMR 3100 (Reporting and Recordkeeping Requirements) (Blackline to reflect non-material changes)

Appendix 3 - Text of Final Amendments to DMR 3100 (Reporting and Recordkeeping Requirements) (Clean)

Appendix 4 – Text of Amendments to section 3703 of the IIROC Rules (Reporting by a Dealer Member to IIROC) (Blackline to reflect non-material changes)

Appendix 5 - Text of Amendments to section 3703 of the IIROC Rules (Reporting by a Dealer Member to IIROC) (Clean)

Appendix 6 – Notice 19-0195 - Frequently Asked Questions – Mandatory Cybersecurity Incident Reporting