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

IIROC NOTICE

Rules Notice
Request for Comments
Dealer Member Rules

Comments Due By: May 22, 2018

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

18-0070
April 5, 2018

Proposed Amendments Respecting Mandatory Reporting of Cybersecurity Incidents

Executive Summary

IIROC is proposing amendments to the Dealer Member Rules (**DMRs**) and corresponding amendments for the proposed IIROC Dealer Member Plain Language Rule Book (the **proposed PLR Rule Book**[1]) to require mandatory reporting of a cybersecurity incident by Dealer Members (**Dealers**) to IIROC (the **Proposed Amendments**). We are introducing the Proposed Amendments because:

- cybersecurity incidents are increasing in frequency and sophistication
- information sharing is an essential tool for mitigating cyber threats.

The Proposed Amendments would:

- require Dealers to promptly report cybersecurity incidents to IIROC
- list the information Dealers must report.

[1] We republished the proposed PLR Rule Book on March 9, 2017 in Notice 17-0054. On January 18, 2018, we published Notice 18-0014, which republished only those sections of the proposed PLR Rule Book with material changes made in response to comments.

As the Proposed Amendments are going through the normal rule-development process, we ask that Dealers continue to voluntarily report to us any cybersecurity incidents as part of their management of cyber risks.

Impacts

We expect Dealers will benefit from the prompt reporting of cybersecurity incidents. When IIROC receives notice of an incident it can move quickly to assist the affected Dealer(s) and, when necessary, inform other Dealers of current cyber threats, thereby helping to manage the impact on Dealers as well as investors. The Proposed Amendments reflect our continued work with Dealers to increase their cybersecurity preparedness.

How to Submit Comments

We request comments on all aspects of the Proposed Amendments, including any matter they do not specifically address. Submit comments on the Proposed Amendments in writing and deliver by ***May 22, 2018*** to:

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

Also, provide a copy to the Recognizing Regulators by forwarding a copy to:

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

Commentators should be aware that a copy of their comment letter will be made publicly available on the IIROC website at www.iiroc.ca.

Rules Notice - Table of Contents

1. Discussion of Proposed Amendments

1.1 Relevant background

Cybersecurity is a key issue for Dealers and IIROC. The active management of cyber risk is critical to the stability of Dealers, the integrity of capital markets and the protection of investors.

Over the past few years, we have committed to helping Dealers strengthen their risk management practices and increase their cybersecurity preparedness. Our work includes:

- in December 2015, publishing two resources, the Cybersecurity Best Practices Guide and the Cyber Incident Management Planning Guide
- in June 2016, coordinating a cybersecurity self-assessment survey completed by all Dealers
- issuing confidential report cards to each Dealer evaluating their cybersecurity practices
- consulting with industry and cybersecurity experts
- connecting IIROC cybersecurity specialists and Dealers that have cybersecurity maturity levels below the expected target of their industry peer group.

On March 22, 2018, we issued Technical Notice 18-0063 in which we:

- noted the increased frequency and sophistication of cybersecurity incidents
- signalled that we were working on the Proposed Amendments
- asked Dealers to promptly report cybersecurity incidents to IIROC in the interim.

Currently, there are no mandatory reporting requirements in the DMRs expressly related to cybersecurity incidents. However, our Cybersecurity Best Practices Guide recommends timely incident reporting as part of firms' cybersecurity policies and some Dealers have voluntarily reported cybersecurity incidents to us. Information sharing is an essential tool for mitigating cyber threats, particularly in a rapidly evolving threat landscape.

1.2 Proposed Amendments

To further support Dealers, and help them in strengthening their management of cyber risks, the Proposed Amendments:

- require Dealers to report cybersecurity incidents to IIROC within three calendar days from discovering the incident
- set out the information Dealers must report to IIROC respecting the incident.

The Proposed Amendments require Dealers submit two reports:

- a report submitted shortly after discovery of the incident
- an incident investigation report submitted 30 days, unless otherwise agreed to by IIROC, after the incident. This report is meant to be more comprehensive and requires information that may not be available immediately after discovery of an incident. The 30-day period

should provide adequate time for a Dealer to undertake and complete an incident investigation to determine, among other things, the cause of the incident.

The text of the Proposed Amendments:

- to the DMRs is set out in **Appendix 1**
- to the proposed PLR Rule Book is set out in **Appendix 2** (blacklined to the January 2018 publication of the PLR Rule Book) and **Appendix 3** (clean).

As the Proposed Amendments are going through the normal rule-development process, we ask that Dealers continue to voluntarily report to us any cybersecurity incidents as part of their management of cyber risks.

2. Analysis

The Proposed Amendments are consistent with similar provisions in federal and provincial privacy legislation, as well as regulations governing financial services implemented in the U.S. We summarize the comparable provisions in this section.

2.1 Federal legislation

Under Canada's *Personal Information Protection and Electronic Documents Act* (**PIPEDA**), organizations must implement policies and practices to protect personal information in their custody or control against loss or theft, as well as unauthorized access, disclosure, copying, use or modification.

In June 2015, the *Digital Privacy Act* amended PIPEDA to require organizations to notify the Privacy Commissioner and affected individuals of:

> any breach of security safeguards involving personal information under the organization's control, if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual.[2]

However, these breach reporting provisions are not yet in force. They will be brought into force only after related regulations outlining specific requirements are developed.

2.2 Provincial legislation

Alberta is the only province whose privacy legislation contains mandatory breach notification requirements. In Alberta, PIPEDA does not apply because the federal government has deemed the province's privacy legislation to be substantially similar to PIPEDA. Alberta's legislation provides as follows:

> 34.1(1) An organization having personal information under its control must, without unreasonable delay, provide notice to the Commissioner of any incident involving the loss of or unauthorized access to or disclosure of the personal information where a

[2] See Amendments Not in Force, section 10.

reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure.

(2) A notice to the Commissioner under subsection (1) must include the information prescribed by the regulations.[3]

Alberta's regulations set out the required elements of the incident notice, as follows:

19 A notice provided by an organization to the Commissioner under section 34.1(1) of the Act must be in writing and include the following information:

(a) a description of the circumstances of the loss or unauthorized access or disclosure;

(b) the date on which or time period during which the loss or unauthorized access or disclosure occurred;

(c) a description of the personal information involved in the loss or unauthorized access or disclosure;

(d) an assessment of the risk of harm to individuals as a result of the loss or unauthorized access or disclosure;

(e) an estimate of the number of individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure;

(f) a description of any steps the organization has taken to reduce the risk of harm to individuals;

(g) a description of any steps the organization has taken to notify individuals of the loss or unauthorized access or disclosure;

(h) the name of and contact information for a person who can answer, on behalf of the organization, the Commissioner's questions about the loss or unauthorized access or disclosure.[4]

2.3 U.S. legislation

The New York State Department of Financial Services (**DFS**) regulates financial services and products in the State of New York. Under the New York State Cybersecurity Regulation, any entity regulated by DFS must:

notify the superintendent as promptly as possible but in no event later than 72 hours from a determination that a Cybersecurity Event has occurred that is either of the following:

(1) Cybersecurity Events impacting the Covered Entity of which notice is required to be provided to any government body, self-regulatory agency or any other supervisory body; or

---

[3] Section 34.1(1) of *Personal Information Protection Act* (2003, Chapter P-6.5).
[4] Section 19 of *Personal Information Protection Act Regulation*, AR 366/2003.

(2) Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity. [5]

A "Cybersecurity Event" is defined as any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an information system or information stored on such information system.[6]

2.4 Issues and alternatives considered

To clarify our expectation that Dealers report cybersecurity incidents to us as part of their management of cyber risk, we considered amending our DMRs, or maintaining the status quo. Our current cybersecurity guides[7] provide comprehensive guidance to Dealers about all elements of a robust cybersecurity program. A model program includes cybersecurity incident reporting. While we expect Dealers to continue to voluntarily report cybersecurity incidents to us, we chose to amend our DMRs because of:

- the growing risk of harm to investors, market participants and Dealers as a result of recent cybersecurity incidents
- the importance of timely information sharing to mitigate this risk.

Prompt cybersecurity incident reporting helps us:

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

3. Impacts of the Proposed Amendments

We expect IIROC, Dealers and their clients to benefit from prompt and mandatory cybersecurity incident reporting to us. As noted above, information sharing is an essential tool for mitigating cyber threats.

The Proposed Amendments do not impose any burden or constraint on competition or innovation that is not necessary to further IIROC's regulatory objectives. The Proposed Amendments may impose some increased costs of compliance but they are consistent with certain current provincial privacy laws and forthcoming federal privacy laws. Accordingly, to the extent Dealers must make changes to their systems, policies and procedures, we expect many Dealers may have already made such changes or are in the process of doing so in preparation for the federal regulations that are to come into effect.

---

[5] Section 500.17 of 23 NYCRR 500 – Cybersecurity Requirements for Financial Services Companies.
[6] Section 500.01(d) of 23 NYCRR 500 – Cybersecurity Requirements for Financial Services Companies.
[7] The Cybersecurity Best Practices Guide and the Cyber Incident Management Planning Guide.

4. Implementation

4.1 Technological Implications

We do not expect the Proposed Amendments to have material technological implications.

4.2 Implementation plan

If approved we anticipate implementing the Proposed Amendments as follows:

- The changes to DMR 3100 will be implemented as soon as our Recognizing Regulators approve them.
- The changes to section 3705 of the proposed PLR Rule Book will be implemented when the proposed PLR Rule Book becomes effective. We will incorporate the Proposed Amendments into the proposed PLR Rule Book when we publish the Notice of Approval.

5. Policy development process

5.1 Regulatory purpose

The purpose of the Proposed Amendments is to:

- foster fair, equitable and ethical business standards and practices
- promote the protection of investors
- mitigate a substantial risk of material harm to investors, market participants and Dealer Members.

5.2 Regulatory process

IIROC's Board of Directors (**Board**) has determined the Proposed Amendments to be in the public interest and on March 28, 2018 approved them for public comment.

After considering the comments received in response to this Request for Comments together with any comments of the Recognizing Regulators, IIROC may recommend revisions to the Proposed Amendments. If the revisions and comments received are not of a material nature, the Board has authorized the President to approve the revisions. The Proposed Amendments as revised will be subject to approval by the Recognizing Regulators. If the revisions or comments are material, we will submit the Proposed Amendments, with revisions if made, to the Board for approval for republication or implementation as applicable.

6. Appendices

Appendix 1 – Text of Proposed Amendments to Dealer Member Rule 3100 (*Reporting and Recordkeeping Requirements*)

Appendix 2 – Text of Amendment to section 3703 of the PLR Rule Book (*Reporting by a Dealer Member to IIROC*) (Blackline)

Appendix 3 – Text of Amendment to section 3703 of the PLR Rule Book (*Reporting by a Dealer Member to IIROC*) (Clean)